

L'URNE EST MORTE ! VIVE LE SHADOWVOTE !

Le manuel de la révolution démocratique

Nour-eddine Khaldi

Édition 2026

L'urne est morte ! Vive le ShadowVote ! — Le manuel de la révolution démocratique

Nour-eddine Khaldi

© Nour-eddine Khaldi, 2026. Tous droits réservés.

Toute reproduction ou représentation, intégrale ou partielle, par quelque procédé que ce soit (texte, extraits, illustrations), est interdite sans l'autorisation écrite de l'auteur, sauf dans les cas prévus par la loi (courtes citations, analyses et revues de presse).

ISBN : [à attribuer lors de la publication]

Dépôt légal : [à effectuer lors de la publication, conformément à la législation en vigueur]

Avertissement. *ShadowVote* est un projet citoyen proposé par l'auteur dans cet ouvrage : un essai et un plan d'action, pas un service déjà en fonctionnement. À la date de publication, aucune pétition, plateforme technique, application ou canal de contact officiel liés à ce projet n'existe : leur éventuelle création est décrite au Chapitre 9 comme une feuille de route à venir, non comme un service disponible immédiatement. Le ShadowVote n'est ni un dispositif électoral officiel ni un substitut au vote tel que défini par le Code électoral français : il s'agit d'une proposition et d'un outil citoyen de vérification, sans valeur légale, qui ne remplace, n'altère ni n'affecte en rien le déroulement, le décompte ou la validité d'un scrutin officiel.

Les statistiques citées sont sourcées lorsque cela est indiqué ; les chiffres marqués [*Estimation*] correspondent à des ordres de grandeur avancés par l'auteur, faute de source publique consolidée, et doivent être lus comme tels.

TABLE DES MATIÈRES

TABLE DES MATIÈRES.....	3
SYNOPSIS.....	5
CHAPITRE 1.....	7
LA TRAHISON DU BULLETIN.....	7
CHAPITRE 2.....	17
LES CINQ FAILLES CRITIQUES.....	17
CHAPITRE 3.....	26
L'IMPASSE TOTALE.....	26
CHAPITRE 4.....	37
LA BLOCKCHAIN POUR TOUS.....	37
CHAPITRE 5.....	52
LE SHADOWVOTE — ARCHITECTURE DU SYSTÈME.....	52
1. Le principe du double-vote de la confiance.....	52
2. Les 5 étapes du vote ShadowVote.....	54
3. Architecture technique du système.....	60
4. Budget réaliste et transparent.....	63
5. Feuille de route technique.....	65
CHAPITRE 6.....	68
SÉCURITÉ, ANONYMAT, ACCESSIBILITÉ.....	68
1. Sécurité : plus robuste que vous ne le craignez.....	69
2. Anonymat : une pseudonymisation forte, pas un secret absolu.....	78
3. Accessibilité : de 7 à 107 ans.....	83
4. Le coût réel.....	86
Conclusion du chapitre : la plupart des objections techniques trouvent une réponse solide.....	88
CHAPITRE 7.....	90
LA DÉMOCRATIE DE L'OMBRE.....	90
CHAPITRE 8.....	100
LE BASCULEMENT DU 1 %.....	100
CHAPITRE 9.....	111
LA FEUILLE DE ROUTE CITOYENNE.....	111
1. Vue d'ensemble : les quatre phases.....	113
2. PHASE 1 : Le Manifeste (0-6 mois).....	113
3. PHASE 2 : Le Prototype (6-18 mois).....	117
4. PHASE 3 : Le Test Pilote (18-30 mois).....	120
5. PHASE 4 : Le Lobbying Politique (30-36+ mois).....	124
6. Gestion des risques.....	125
7. Plan B : si le ShadowVote échoue.....	126
Conclusion du chapitre : le plan est prêt.....	126
PARTIE IV.....	127
CHAPITRE 10.....	128
VOUS ÊTES LA RÉVOLUTION.....	128
1. Les cinq actions concrètes (à faire maintenant).....	129

2. Devenir Sentinelle : le mode d'emploi.....	133
3. Les slogans du mouvement.....	135
4. Les événements à organiser.....	136
5. La timeline personnelle (vos six prochains mois).....	137
6. Le kit de conversation (pour convaincre).....	137
7. Le créateur qui s'efface : pourquoi je ne dirigerai pas ShadowVote. .	138
8. Conclusion : l'acte fondateur.....	140
ANNEXE A — PROPRIÉTÉ INTELLECTUELLE.....	140
ANNEXE B — RÉFÉRENCES.....	141
À PROPOS DE L'AUTEUR.....	141

SYNOPSIS

En 2026, vous pouvez tracer un colis à 12 000 km, mais pas votre bulletin de vote.

28 % d'abstention. 78 % de défiance. Une génération entière qui décroche.

Et si la solution existait déjà ?

ShadowVote propose une révolution : un vote citoyen parallèle sur blockchain, très difficile à falsifier et vérifiable par tous.

Ce manifeste vous explique :

- Pourquoi notre démocratie est en panne
- Comment la blockchain peut la réparer
- Quand le basculement va se produire
- Comment vous pouvez agir MAINTENANT

Plus qu'un livre, c'est un plan d'action.

Après lecture : impossible de rester passif.

« Ne crois plus, vérifie. » — le slogan du mouvement.

La révolution commence avec vous.

CHAPITRE 1

LA TRAHISON DU BULLETIN

1. Le monde où tout est traçable... sauf votre vote

Faisons un test simple.

Ouvrez votre application bancaire. Regardez votre dernier achat. Vous voyez :

- La date exacte (jusqu'à la seconde)
- Le lieu précis (nom du commerçant, ville)
- Le montant exact
- Le type de paiement (carte, virement, prélèvement)
- Un numéro de transaction unique
- Un historique consultable à l'infini

Vous pouvez contester. Vous pouvez archiver. Vous pouvez vérifier.

Maintenant, allez sur le site de votre transporteur préféré. Entrez le numéro de suivi de votre dernier colis. Vous voyez :

- Expédié depuis Shanghai le 12/11 à 08h23
- Arrivé à Roissy le 14/11 à 14h07
- En transit vers Lyon le 15/11 à 06h45
- En cours de livraison le 16/11 à 09h12
- Livré chez vous le 16/11 à 11h34
- Signature : « Déposé boîte aux lettres »

Vous avez suivi votre colis à travers deux continents. En temps réel.

Ouvrez votre dossier médical en ligne (Mon espace santé, Ameli). Vous voyez :

- Vos consultations des dix dernières années
- Vos ordonnances archivées
- Vos résultats d'analyses
- Vos vaccinations
- Vos comptes rendus médicaux

Tout est là. Sécurisé. Crypté. Accessible.

L'expérience qui révèle tout

Maintenant, essayez ceci : cherchez la preuve que votre bulletin de vote du dernier scrutin a été compté.

Allez-y. Essayez.

Vous ne trouverez rien.

- Pas de numéro de suivi
- Pas de confirmation
- Pas d'historique
- Pas de trace

Rien.

Le paradoxe insupportable

Voici le paradoxe insupportable de notre époque :

TABLEAU — CE QUE VOUS POUVEZ VS NE POUVEZ PAS VÉRIFIER

Ce que vous POUVEZ vérifier	Ce que vous NE POUVEZ PAS vérifier
Un virement de 5 €	Votre vote à la présidentielle
Un colis à 12 000 km	Le décompte de votre bureau de vote
Une pizza livrée à domicile	Les résultats nationaux
Un email gratuit	L'acte démocratique le plus important
Votre dossier médical	La légitimité de vos représentants

Vous pouvez tout tracer, sauf l'essentiel.

L'aberration technologique

Cette aberration n'est pas un détail. C'est le symptôme d'une maladie profonde. Et disons-le tout de suite, pour que les choses soient claires dès la première page : ce n'est pas parce que quelqu'un truque les comptes. C'est parce que personne, pas même vous, ne peut vérifier qu'ils sont justes. Nous y reviendrons. Retenez seulement ceci pour l'instant : la trahison dont ce livre parle n'est pas celle d'un tricheur. C'est celle d'un système qui ne vous laisse pas le choix de le croire sur parole ou de le vérifier.

En 2026, nous avons la technologie pour :

- Sécuriser des centaines de millions de paiements chaque jour
- Tracer des millions de colis à travers la planète
- Gérer des milliers de milliards d'euros avec une traçabilité complète
- Protéger des données médicales sensibles de millions de citoyens

Mais nous votons encore comme en 1913.

Du papier. Une urne transparente. Des bénévoles fatigués. Un dépouillement manuel. Et une seule garantie : la foi aveugle en l'institution.

2. Les chiffres qui font mal

La crise n'est pas une impression. C'est un fait mesurable.

France : l'effondrement de la participation

TABLEAU — ABSTENTION PRÉSIDENTIELLES (SECOND TOUR)

Année	Taux d'abstention	Évolution
1965	15,7 %	Base
1981	14,1 %	-1,6
1995	20,3 %	+6,2
2002	20,3 %	=
2007	16,0 %	-4,3
2012	19,7 %	+3,7
2017	25,4 %	+5,7
2022	28,0 %	Record historique

Source : ministère de l'Intérieur, résultats officiels du second tour.

La catastrophe législative

Élections législatives 2022 :

- Abstention au premier tour : **52,5 % — record pour un premier tour sous la Ve République**
- Abstention au second tour : **près de 54 %**

Traduction concrète : en 2022, plus d'un électeur sur deux n'a pas pris part au choix de son député. En 2024, après la dissolution, la participation a fortement rebondi (66,7 % au premier tour) — preuve que les citoyens reviennent aux urnes quand ils sentent que leur voix pèse.

Source : ministère de l'Intérieur, résultats officiels des législatives 2022 et 2024.

L'Europe qui décroche

Élections européennes 2024 : abstention France, **48,5 %**. Près d'un Français sur deux n'a pas voté.

Source : Parlement européen, résultats définitifs (participation en France : 51,49 %).

La fracture générationnelle

TABLEAU — PARTICIPATION PAR TRANCHE D'ÂGE (PRÉSIDENTIELLE 2022, SECOND TOUR)

Tranche d'âge	Taux de participation	Abstention
70 ans et +	85 %	15 %

60-69 ans	80 %	20 %
50-59 ans	74 %	26 %
35-49 ans	65 %	35 %
25-34 ans	62 %	38 %
18-24 ans	59 %	41 %

Source : Ipsos / Sopra Steria, enquête du 21 au 23 avril 2022 auprès de 4 000 inscrits (sondage : estimations).

Révélation choc : même à la présidentielle, l'élection qui mobilise le plus, 41 % des 18-24 ans sont restés chez eux — près de trois fois plus que les plus de 70 ans. Aux autres scrutins, plus d'un jeune sur deux ne vote plus : 71 % d'abstention chez les 18-24 ans au second tour des législatives 2022, environ 60 % aux européennes 2024, 56 % au premier tour des municipales 2026 (enquêtes Ipsos). Une génération entière est en train de décrocher de la démocratie — la même génération qui vérifie en un geste le solde de son compte, le statut de sa commande et l'état de sa carte Vitale. Ce n'est peut-être pas un hasard. Nous y reviendrons dans les portraits qui suivent.

Europe : une pandémie démocratique

TABLEAU — ABSTENTION MOYENNE, ÉLECTIONS LÉGISLATIVES NATIONALES (2015-2024)

Pays	Abstention moyenne
Suisse	45 %
Portugal	43 %
Pologne	40 %
Royaume-Uni	33 %
Allemagne	24 %

[Estimation] — moyenne indicative construite à partir des taux de participation nationaux publiés sur la période ; à consolider pays par pays avec les instituts électoraux nationaux ou International IDEA avant toute citation hors de cet ouvrage.

TABLEAU — ABSTENTION AUX ÉLECTIONS EUROPÉENNES 2024

Pays	Abstention
Croatie	78,7 %
Lituanie	71,0 %
Slovaquie	65,6 %
Tchéquie	63,6 %
France	48,5 %

Source : Parlement européen, résultats définitifs 2024 (abstention = 100 – participation). Moyenne de l'Union : 49,3 %.

États-Unis : un électeur sur trois reste chez lui

TABLEAU — PARTICIPATION PRÉSIDENTIELLES USA

Année	Taux de participation
2016	61,4 %
2020	66,8 % (pic exceptionnel)
2024	65,3 %

Élections de mi-mandat (midterms) : **53,4 % en 2018, 52,2 % en 2022.**

Source : US Census Bureau, enquête Current Population Survey (taux rapporté aux citoyens en âge de voter). Même lors d'une présidentielle très mobilisatrice, un Américain sur trois ne vote pas.

La défiance mesurée

Chaque année, le baromètre de la confiance politique du Cevipof (Sciences Po) mesure la confiance des citoyens dans la politique, en France et chez nos voisins.

TABLEAU — CITOYENS QUI N'ONT PAS CONFIANCE DANS LA POLITIQUE (JANVIER 2026)

Pays	N'ont pas confiance	Écart avec la France
France	78 %	—
Italie	60 %	18 points de moins
Royaume-Uni	56 %	22 points de moins
Allemagne	55 %	23 points de moins

Source : Cevipof / OpinionWay, Baromètre de la confiance politique, vague 2026 (terrain du 12 au 28 janvier 2026, 3 166 inscrits en France).

À ce chiffre s'ajoute une seconde mesure, distincte, qu'il ne faut pas confondre avec la précédente : en France, **76 % des citoyens jugent que la démocratie fonctionne mal** (même source) — un niveau historiquement bas. Une chose est de ne plus faire confiance aux responsables politiques ; une autre est de douter que le système lui-même tienne ses promesses. Les deux courbes pointent dans la même direction. Ce chiffre n'est pas anecdotique. C'est une alerte rouge.

3. Portraits d'abstentionnistes

Les statistiques sont froides. Mettons des visages sur ces chiffres. Les quatre portraits qui suivent sont des personnages composites, inspirés de propos fréquemment entendus : ils ne désignent aucune personne réelle.

Martine, 68 ans, retraitée — Rouen

« J'ai voté toute ma vie, depuis mes 18 ans. J'y allais comme on va à la messe. C'était sacré. Mais en 2022, pour la première fois, je suis restée chez moi.

Pourquoi ? Parce que je ne crois plus que ça change quoi que ce soit. Ils promettent, ils promettent, et après rien ne bouge. Pire : des fois, je me demande si nos votes sont vraiment comptés comme il faut.

L'autre jour, j'ai vu passer une info comme quoi, quelque part en France, on avait retrouvé des bulletins oubliés dans un sac après le dépouillement. Je ne saurais même pas vous dire où ni combien exactement. Mais ça m'est resté. Et combien de fois ça arrive sans qu'on le sache ?

Alors à quoi bon ? Je préfère garder mon énergie pour mes petits-enfants. »

Martine n'est pas complotiste. Elle ne pense pas que les élections sont « truquées ». Elle pense juste que ça ne sert à rien, et qu'elle n'a de toute façon aucun moyen de savoir si elle a tort. Elle a tenu ce raisonnement à distance pendant près de cinquante ans. Et des Martine, il y en a des millions.

Julien, 31 ans, développeur informatique — Lyon

« Franchement, aujourd'hui, on me demande de mettre un papier dans une boîte ? Sérieux ?

Je gère des millions de transactions par jour sur des serveurs sécurisés. Je fais des virements instantanés avec mon téléphone. Et pour voter, je dois me déplacer un dimanche, faire la queue, et lâcher un bout de papier dans un trou ?

C'est ridicule. Si le système était digne du XXI^e siècle, je voterais peut-être. Mais là, c'est comme si on me demandait d'envoyer un fax pour commander sur Amazon.

Et en plus, impossible de vérifier quoi que ce soit. Dans mon métier, tout est auditable, tout est tracé, tout est prouvable. Le vote ? C'est une boîte noire totale.

Donc non, merci. Je signe des pétitions en ligne, je fais des dons à des associations, je débats sur les réseaux. Mais l'urne ? C'est un vestige du passé. »

Julien n'est pas désengagé. Il est hyper-connecté. Mais le système électoral lui paraît archaïque. Et il a raison.

Inès, 24 ans, étudiante — Marseille

« Honnêtement, je ne sais même pas pour qui voter.

Ils disent tous la même chose. Ils se critiquent entre eux. Et après l'élection, c'est toujours pareil. Mon grand-père me dit que je dois voter « pour ceux qui se sont battus pour ce droit ». Je comprends.

Mais moi, j'ai l'impression que mon vote ne pèse rien. Un bulletin parmi des dizaines de millions ? C'est une goutte dans l'océan.

Et puis, comment je sais qu'il a été compté ? On me dit « fais-nous confiance ». Mais pourquoi je ferais confiance à un système que je ne peux pas vérifier ?

Quand je transfère de l'argent à une amie avec une appli, je reçois une confirmation instantanée. Quand je vote, je reçois... rien. Juste « merci d'être venue ».

Donc voilà. En 2027, j'irai peut-être. Ou peut-être pas. On verra. »

Inès n'est pas apolitique. Elle manifeste pour le climat. Elle s'indigne sur les réseaux sociaux. Mais le vote ? Elle n'y croit pas. Et elle n'est pas seule : aux municipales de 2026, 56 % des 18-24 ans ne sont pas allés voter.

Thomas, 52 ans, ouvrier — Valenciennes

« Moi, je ne vote plus depuis 2017.

J'avais voté au premier tour pour un candidat qu'on m'avait présenté comme un rempart, quelqu'un de sérieux, de solide. Et puis il y a eu une affaire, un scandale qui a éclaboussé ses proches. Je me suis senti trahi. Après, on m'a dit : votez pour l'autre, celui d'en face, pour faire barrage. J'ai voté, comme on appelle les pompiers en dernier recours.

Et qu'est-ce que ça a donné, une fois l'élu en poste ? Des prélèvements qui ont tapé directement sur la fiche de paie de ma mère retraitée. Des services publics fermés les uns après les autres dans ma région — l'hôpital, la poste, l'école du village. Et quand des gens comme moi sont descendus dans la rue pour le dire, on nous a traités comme des délinquants.

Alors maintenant, je ne crois plus personne. Qu'ils se débrouillent sans moi.

Et puis, entre nous, comment on sait que les votes sont bien comptés ? Moi, mon bulletin, une fois qu'il est dans l'urne, il pourrait aussi bien finir à la poubelle, je n'en saurais rien.

Tant qu'on ne pourra pas vérifier, je ne jouerai plus à leur jeu. »

Thomas n'est pas apathique. Il travaille, il paie ses impôts, il suit l'actualité. Mais voter ? Il n'y croit plus.

4. Le certificat aveugle

Ces quatre témoignages ont un point commun.

Aucun de ces citoyens n'affirme que les élections sont truquées. Ils disent juste : « Je ne peux pas vérifier. Donc je ne crois plus. »

C'est ce que nous appelons **le certificat aveugle**.

L'analogie bancaire révélatrice

Quand vous votez, on vous donne un récépissé. Un petit papier qui dit : « Vous avez voté. »

Mais ce récépissé ne prouve rien.

- Il prouve que vous êtes venu
- Il prouve que vous avez signé
- Il prouve que vous avez glissé une enveloppe
- Il ne prouve pas que votre bulletin a été compté

C'est comme si votre banque vous disait : « Merci d'avoir déposé votre argent. Nous l'avons bien reçu. Mais non, vous ne pouvez pas consulter votre compte. Non, nous ne vous enverrons pas de relevé. Non, vous ne pourrez pas vérifier vos transactions. Juste... faites-nous confiance. »

Vous changeriez de banque immédiatement.

La foi aveugle exigée

Pourtant, c'est exactement ce qu'on vous demande avec le vote.

Faites-nous confiance. Faites confiance aux assesseurs, que vous ne connaissez pas. Faites confiance au processus de centralisation, que vous ne voyez pas. Faites confiance aux chiffres annoncés, que vous ne pouvez pas auditer. Faites confiance. Point.

La cécité organisée

Et le pire, c'est que cette cécité n'est pas un bug. C'est une fonctionnalité.

Le système vous demande un acte de foi envers une institution qui refuse toute vérification individuelle. Votre certificat de vote est aveugle : il prouve que vous avez voté, pas que votre vote a été comptabilisé correctement.

5. Le premier acte de renoncement

Accepter le certificat aveugle, c'est accepter l'opacité. C'est renoncer à vérifier. C'est renoncer à savoir. C'est renoncer à prouver. C'est le premier acte de soumission démocratique.

Martine l'a accepté pendant près de cinquante ans. Puis elle a craqué.

Julien refuse de l'accepter. Il préfère s'abstenir.

Inès hésite. Elle sent que quelque chose ne va pas.

Thomas l'a accepté une fois de trop. Il ne reviendra plus.

La question qui vous concerne

Et vous ?

Combien de fois avez-vous accepté de voter sans pouvoir vérifier ? Combien de fois avez-vous glissé votre bulletin dans l'urne en vous disant : « J'espère qu'il sera bien compté » ? Combien de fois avez-vous regardé les résultats à la télévision en vous demandant : « Est-ce vraiment ça, ou... ? »

Ce doute, aussi minime soit-il, est le poison qui tue la démocratie. Pas les fraudes massives, qui restent rares. Pas les manipulations flagrantes, qui sont minoritaires. Juste le doute. Le doute qui s'installe. Le doute qui grandit. Le doute qui, lentement mais sûrement, vide l'urne de sa légitimité.

Ce poison a ceci de particulier qu'il ne se guérit pas en jurant, la main sur le cœur, qu'il n'y a pas de fraude. On ne rassure pas quelqu'un qui doute en lui redisant « fais-moi confiance » : c'est justement la phrase qui a déclenché le doute. Il faut autre chose. C'est ce que ce chapitre va maintenant établir.

6. La trahison n'est pas la fraude

Soyons clairs, tout de suite, avant d'aller plus loin.

Ce livre n'affirme pas que les élections françaises sont truquées. Ce serait malhonnête. Les cas avérés de fraude massive sont rares. Le système, dans son ensemble, fonctionne relativement bien.

Mais « relativement bien » ne suffit plus, pour une raison précise qu'il faut nommer.

La différence entre douter d'un homme et douter d'un système

Il y a deux façons bien différentes de perdre confiance dans une élection. La première, c'est de croire qu'on vous a menti — qu'un scrutateur a triché, qu'un chiffre a été maquillé. C'est grave, mais c'est un problème d'hommes : on peut chercher le coupable, le juger, le sanctionner.

La seconde façon, plus discrète et plus corrosive, c'est de réaliser qu'on ne pourrait de toute manière rien vérifier, même si on le voulait — qu'il n'y a personne à accuser parce que le système lui-même n'a pas été conçu pour apporter une preuve individuelle. Ce n'est plus une question de confiance envers des personnes. C'est une question de conception.

C'est cette seconde trahison qui traverse ce chapitre. La trahison du bulletin n'est pas la fraude. C'est l'impossibilité de vérifier. C'est cette seconde où votre enveloppe tombe dans l'urne et où vous perdez tout contrôle. C'est ce moment où votre voix, la chose la plus précieuse en démocratie, disparaît dans une boîte noire. C'est ce système qui vous dit : « Crois, ne vérifie pas. »

Regardez à nouveau les tableaux de ce chapitre : Croatie, Lituanie, Slovaquie, République tchèque, États-Unis. Aucun de ces pays ne fait mieux que la France sur ce point précis. Dans aucun d'eux, un citoyen ne peut, seul, prouver que son bulletin a été comptabilisé. Même l'Estonie, pionnière

du vote par Internet, ne permet à l'électeur que de vérifier, pendant un court délai, que son vote a bien été reçu — pas qu'il a été correctement compté. Ce n'est donc pas une pathologie française. C'est un angle mort universel, hérité d'une même origine : des systèmes de vote conçus au XIXe siècle, quand la vérification individuelle était techniquement impossible, et jamais repensés depuis, alors que la vérification est devenue techniquement triviale.

C'est ça, la trahison. Pas une trahison des hommes. Une trahison du système.

Conclusion du chapitre

Le certificat aveugle est le symbole de cette trahison, et il fonctionne comme un engrenage : tant que vous acceptez de voter sans pouvoir vérifier, vous validez l'opacité ; tant que vous acceptez le « faites-nous confiance », vous renoncez à votre souveraineté. Ce renoncement est la première faille mortelle de notre système électoral.

Ce n'est que la première. Dans le prochain chapitre, nous allons décortiquer les quatre autres — celles qui touchent, non plus à votre expérience individuelle de citoyen, mais à l'architecture même de l'urne : sa centralisation, sa lenteur, son coût, et sa fragilité face à un monde qui a changé de siècle sans elle.

Nous allons comprendre pourquoi le système est structurellement incapable de restaurer seul la confiance qu'il a perdue. Et nous allons poser une question simple : si le système ne peut pas se réformer de l'intérieur, que nous reste-t-il ?

Vous venez de voir l'ampleur du problème. Maintenant, découvrons ensemble la solution qui va tout changer.

CHAPITRE 2

LES CINQ FAILLES CRITIQUES

« Ce n'est pas parce qu'un système a fonctionné pendant un siècle qu'il doit fonctionner pendant un siècle de plus. »

1. Une invention plus récente qu'on ne le croit

L'isoloir et l'enveloppe que vous connaissez n'ont pas toujours existé.

Beaucoup pensent que le vote secret est aussi vieux que la République elle-même. C'est presque vrai — mais pas tout à fait. Et cette nuance change tout.

1848 : l'universel, mais pas encore le secret

En 1848, la France instaure le suffrage universel — masculin. C'est une avancée considérable pour l'époque.

L'année où Karl Marx publie le *Manifeste du Parti communiste*. L'année où la France abolit l'esclavage. Une époque sans éclairage électrique, sans téléphone, sans automobile.

Mais voter en 1848, ce n'est pas voter comme aujourd'hui. Il n'y a ni isoloir, ni enveloppe neutre. Les bulletins sont souvent imprimés par les partis eux-mêmes, dans des formats ou des couleurs différents : impossible de cacher son choix à qui regarde par-dessus votre épaule. Le geste du vote reste, dans les faits, un acte public.

- Les riches votent devant tout le monde.
- Les pauvres sont intimidés.
- Les patrons surveillent leurs ouvriers.

Le suffrage est universel sur le papier. Il reste, dans la pratique, une démonstration publique de loyauté.

1913 : la vraie révolution du vote secret

Il faudra attendre soixante-cinq ans de plus — et la loi du 29 juillet 1913 — pour que la République se dote enfin des outils du vote réellement secret :

- **L'isoloir**, pour se soustraire aux regards.
- **L'enveloppe**, uniforme pour tous, pour masquer le choix jusqu'à l'ouverture.
- **L'urne**, dont la transparence sera plus tard imposée par la loi (article L. 63 du Code électoral), pour garantir qu'aucun bulletin n'y ait été glissé avant l'heure.

C'était génial. Pour la première fois, un ouvrier pouvait voter contre son patron sans que personne ne le sache. Pour la première fois, le vote devenait vraiment libre — et pas seulement universel.

Ce n'est donc pas 1848 qu'il faut retenir, mais 1913. Et ce n'est pas un détail d'historien : c'est un argument. Le système que nous utilisons aujourd'hui a déjà été profondément réformé une fois, pour répondre aux failles de son époque. Rien n'interdit — rien n'empêche — qu'il le soit une seconde fois.

Un succès historique

Pendant plus d'un siècle, ce système a bien fonctionné.

Il a permis des alternances. Il a élu des présidents. Il a fait vivre la démocratie.

Mais nous ne sommes plus en 1913.

2. Les cinq failles critiques du système actuel

Le vote par urne repose sur trois piliers fragiles :

- **La confiance aveugle** (« Faites-nous confiance, on compte bien »)
- **L'impossibilité de vérifier** (une fois votre bulletin dans l'urne, vous ne savez plus rien)
- **Le comptage manuel** (les humains s'épuisent, se trompent, peuvent tricher)

En 1913, on n'avait pas le choix. Mais aujourd'hui, on a la technologie pour faire infiniment mieux.

Ces trois piliers ne sont pas de simples défauts théoriques : sur le terrain, ils se traduisent concrètement par cinq failles précises, que nous allons examiner une par une. Elles ne remplacent pas les trois piliers — elles en sont la manifestation pratique, l'addition de leurs conséquences dans l'isoloir, sur la table de dépouillement, et jusque dans le bureau où l'on proclame les résultats.

FAILLE #1 : L'impossibilité de vérifier

Vous glissez votre bulletin dans l'urne.

Question : comment savez-vous qu'il a été compté ?

Réponse : vous ne le savez pas.

Vous ne pouvez pas retrouver votre bulletin — il est anonyme. Vous pouvez certes assister au dépouillement de votre bureau, mais pas à celui des quelque 69 000 autres bureaux de vote du pays. Et une fois les résultats proclamés, plus rien n'est vérifiable par vous.

Vous devez juste y croire.

L'analogie révélatrice

Dans n'importe quel autre domaine, ce serait inacceptable.

Service	Niveau de vérification	Vote
À la banque — « Votre virement est parti »	Reçu instantané, historique complet, tout vérifiable	AUCUN — « Faites-nous confiance »
À La Poste — « Votre colis est expédié »	Numéro de suivi, géolocalisation, traçage en temps réel	AUCUN — « Croyez-nous »
Sur Amazon — « Commande validée »	Confirmation, suivi, preuve de livraison, chaque étape visible	AUCUN — « On vous promet »

Vous refuseriez immédiatement ces conditions dans n'importe lequel de ces contextes. Pourtant, pour le vote — l'acte démocratique le plus important — on vous demande exactement ça : « Votez. Et faites-nous confiance. »

FAILLE #2 : Les erreurs de comptage documentées

Les assesseurs sont des bénévoles. Parfois âgés. Toujours humains. Et les humains font des erreurs.

Type d'incident (cas génériques, contentieux électoral français)	Erreur	Impact
Municipales	Bulletins retrouvés hors de l'urne après la clôture du scrutin	Premier tour annulé dans le bureau concerné
Législatives	Bulletins présents dans l'urne avant l'ouverture officielle du bureau	Résultat invalidé dans les bureaux concernés
Tous scrutins	Erreurs de décompte	Recomptages demandés

Ces trois types d'incidents sont des schémas récurrents du contentieux électoral français plutôt que des cas isolés attribués ici à une commune précise — un lecteur souhaitant des décisions nominatives peut les rechercher dans la jurisprudence du Conseil d'État en matière électorale.

Le calcul qui fait peur

Question : combien d'erreurs se glissent dans les dizaines de millions de bulletins comptés à la main à chaque élection nationale ?

Réponse : personne ne le sait précisément. On ne recompte presque jamais.

Estimation conservatrice [Estimation] : si l'on ne se trompait que dans 0,1 % des cas — une erreur pour mille bulletins — cela représenterait, à l'échelle d'une élection présidentielle, plusieurs dizaines de milliers de bulletins mal comptés.

Et dans les scrutins locaux, qui se jouent parfois à quelques voix près, quelques erreurs suffisent à changer le résultat — c'est d'ailleurs pour cela que le juge électoral annule régulièrement des élections municipales serrées.

FAILLE #3 : La fraude est possible et documentée

Ne soyons pas naïfs. La fraude existe.

Pas une fraude massive organisée à l'échelle nationale — ça, c'est du complotisme. Mais des petites fraudes locales, documentées, avérées.

Type de fraude	Méthode	Exemple documenté ou fréquence	Ce que prévoit la loi
Achat de votes	Argent ou avantages contre un bulletin	Corbeil-Essonnes : municipales de 2008 annulées par le Conseil d'État (8 juin 2009) en raison de dons d'argent	Jusqu'à 2 ans de prison et 15 000 € d'amende (art. L. 106 du Code électoral)
Fraude au dépouillement	Bulletins soustraits ou cachés	Perpignan : « fraude à la chaussette », municipales de 2008 annulées (Conseil d'État, 23 avril 2009)	1 an de prison et 15 000 € d'amende, peine doublée pour un président de bureau de vote (art. L. 113)
Procurations frauduleuses	Procurations au nom de personnes absentes ou décédées	Affaires jugées régulièrement [ordre de grandeur : aucune statistique officielle consolidée]	Mêmes peines (art. L. 113 et L. 116), et inéligibilité possible (art. L. 117)
Irrégularités de bureau	Urne non verrouillée,	Présidentielle 2022 :	Annulation des suffrages

	assesseurs absents, procès- verbal non transmis	irrégularités relevées dans 45 bureaux sur 69 242 ; 19 960 suffrages annulés par le Conseil constitutionnel	concernés
Destruction ou altération de bulletins	Lors du dépouillement	Cas rares mais avérés	Art. L. 113 et L. 116

Sources : Conseil d'État, 8 juin 2009 (Corbeil-Essonnes) et 23 avril 2009 (Perpignan) ; Conseil constitutionnel, proclamation des résultats de l'élection présidentielle de 2022 ; Code électoral. Aucun organisme ne publie de statistique consolidée de la fraude électorale locale : les cas connus sont ceux que la justice a eu à juger.

Un schéma qui revient régulièrement : les procurations frauduleuses. Dans plusieurs affaires jugées en France ces dernières années, des procurations ont été établies au nom de personnes décédées ou absentes, qui se sont donc retrouvées à « voter » sans le savoir. Les décisions de justice varient selon les cas : annulation partielle du scrutin concerné, amendes, parfois peines de prison avec sursis pour les organisateurs.

Mais combien de fraudes ne sont jamais détectées ?

Un mot, ici, sur le type d'incident cité plus haut, à la Faille #2 : des bulletins déjà présents dans l'urne avant l'ouverture du bureau. Négligence ou manœuvre délibérée ? Selon les cas, la justice tranche différemment — et c'est précisément le problème : rien, dans le système actuel, ne permet à un citoyen de distinguer par lui-même une erreur d'une fraude. Un système où cette distinction dépend entièrement d'une procédure judiciaire longue et incertaine n'est pas un système fiable. Il est simplement opaque.

FAILLE #4 : L'opacité totale du système

À la clôture du scrutin — 18 heures dans la plupart des communes, jusqu'à 20 heures dans les grandes villes —, les urnes sont vidées sur des tables. Les scrutateurs comptent à la main, en faisant des tas. En théorie, le dépouillement est public : vous avez le droit d'y assister, et même d'y participer comme scrutateur. En pratique, presque personne n'y va, et nul ne peut être présent dans plus d'un bureau à la fois. Vous rentrez chez vous, vous allumez la télévision. On vous annonce les résultats. Et vous devez y croire.

L'illusion de la surveillance

« Mais il y a des assesseurs de tous les partis ! »

C'est vrai. Mais tous les petits partis n'ont pas d'assesseurs partout. Les assesseurs sont fatigués après une longue journée de présence. Les erreurs de comptage ne sont pas toujours intentionnelles. Et le citoyen lambda, qui n'assiste pas au dépouillement, ne vérifie rien.

L'opacité reste totale pour la quasi-totalité des électeurs.

FAILLE #5 : L'impossibilité d'auditer

Imaginez qu'on découvre une fraude. Que fait-on ? On recompte.

Mais recompter quoi ? En France, une fois le dépouillement terminé, les bulletins valables sont détruits en présence des électeurs ; seuls les bulletins blancs, nuls ou contestés sont annexés au procès-verbal (article R. 68 du Code électoral). Un recomptage complet après coup est donc, le plus souvent, matériellement impossible. Il n'y a pas de trace numérique. Pas d'historique inaltérable. Il reste un procès-verbal. C'est tout.

Le contraste avec le système bancaire

En informatique, on appelle ça un système non auditable. Vous ne pouvez pas remonter dans le temps. Vous ne pouvez pas vérifier l'intégrité des données. Vous ne pouvez pas prouver qu'il n'y a pas eu de manipulation.

C'est exactement le contraire de ce qu'on fait pour l'argent. Votre banque conserve un historique de toutes vos transactions : inaltérable, horodaté, vérifiable.

Pourquoi pas pour le vote ?

3. Le vote, un acte moins sécurisé que votre pizza

Reprenons l'exemple du Chapitre 1.

Étape	Pizza à 12 €	Vote présidentiel
Commande	Trace numérique	Bulletin papier
Confirmation	SMS	Aucune
Préparation	« Votre pizza est au four »	Aucun suivi
Livraison	Géolocalisation en temps réel	Aucune trace
Réception	Preuve de livraison	Aucune preuve
Contestation	Possible si erreur	Impossible

Résultat : six niveaux de vérification pour une pizza. Zéro niveau pour l'avenir du pays.

La réalité absurde

Soyons honnêtes : c'est absurde. On sécurise mieux une pizza qu'une élection présidentielle. On trace mieux un colis à 5 € qu'un bulletin de vote.

Est-ce normal ?

4. « Mais ça a toujours fonctionné comme ça ! »

C'est l'argument qu'on entend souvent. « Le vote papier, ça marche depuis plus d'un siècle. Pourquoi changer ? »

Réponse simple : parce que le monde a changé.

L'évolution de la confiance

En 1913, les gens faisaient confiance aux institutions. Pourquoi ? Parce qu'ils n'avaient pas le choix. Pas d'alternative. Pas de technologie pour vérifier. On devait faire confiance.

Mais aujourd'hui :

- On peut vérifier nos transactions bancaires en temps réel.
- On peut suivre nos colis à travers le monde.
- On peut consulter nos données médicales en ligne.
- On peut consulter nos déclarations d'impôts sur un portail officiel.

On peut tout vérifier. Sauf notre vote.

Le décalage générationnel

Résultat : les citoyens du XXI^e siècle ne comprennent plus pourquoi le vote est le seul acte important qu'ils ne peuvent pas vérifier.

Et ils ont raison de ne pas comprendre.

5. Les tentatives de modernisation qui ont échoué

« Mais on a essayé les machines à voter ! »

Oui. Et pourtant, ce fut un échec. Voici ce qui s'est passé.

Les machines à voter en France : un fiasco total

Autorisées par la loi depuis 1969, les machines à voter électroniques se diffusent au milieu des années 2000 dans plusieurs dizaines de communes, notamment lors de la présidentielle de 2007.

Problème	Impact	Coût
Opacité totale	Code source fermé, impossible à auditer par les citoyens	Confiance faible
Lenteur	Temps d'attente allongés dans les bureaux équipés	Contestations
Coût élevé pour les	De 4 000 à 6 000 €	Budgets communaux

communes	par machine (estimation du ministère de l'Intérieur, 2007), plus l'entretien et le stockage	
Vulnérabilités de sécurité	Failles démontrées publiquement par des chercheurs indépendants à l'étranger (Pays-Bas, 2006)	Sécurité mise en doute
Pas de trace papier	Impossible de recompter	Vérification nulle

Résultat : un moratoire est décidé en 2008. Aucune nouvelle commune ne peut s'équiper, et une soixantaine de communes seulement utilisent encore leurs machines (66 en 2019, selon le ministère de l'Intérieur). Dès 2007, le Conseil constitutionnel avait relevé que ces machines rompent le lien symbolique entre le citoyen et son vote.

Pourquoi ça a raté ? Parce qu'on a remplacé l'opacité du papier par l'opacité du logiciel. On a juste déplacé le problème : au lieu de faire confiance aux assesseurs, il fallait faire confiance à une machine dont personne ne connaissait le code.

Ce n'était pas de la modernisation. C'était juste une nouvelle boîte noire.

Retenons la leçon : la technologie ne suffit pas si elle reste fermée. Une solution qui remplace un système opaque par un autre système opaque ne résout rien — elle déplace le problème. C'est précisément ce point que la suite de ce livre devra démontrer autrement.

6. Ce dont on a vraiment besoin

Pour que le vote retrouve la confiance, il faut trois conditions fondamentales.

1. La transparence. Tout le monde doit pouvoir vérifier le décompte. Pas juste les assesseurs. Pas juste les partis — qui peuvent déjà, comme le prévoit le Code électoral, déléguer des représentants pour assister aux opérations de vote et de dépouillement. Tout le monde.

2. La traçabilité. Chaque citoyen doit pouvoir confirmer que son vote a été enregistré. Pas savoir pour qui il a voté — l'anonymat reste garanti. Mais savoir que son bulletin compte.

3. L'inaltérabilité. Une fois le vote enregistré, personne ne doit pouvoir le modifier. Ni un hacker. Ni un fraudeur. Ni un gouvernement. Personne.

Le verdict sur le système actuel

Le système actuel n'offre aucune de ces trois conditions :

- L'urne n'est pas transparente : vous ne voyez pas le comptage.
- Elle n'est pas traçable : impossible de vérifier votre bulletin.
- Elle n'est pas inaltérable : on peut bourrer, détruire, mal compter.

Alors comment faire ?

7. La technologie existe déjà

La bonne nouvelle, c'est qu'on n'a pas besoin d'inventer quoi que ce soit. La technologie existe. Elle est mature. Elle fonctionne.

Elle s'appelle la blockchain.

Une technologie éprouvée

C'est la technologie qui fait fonctionner depuis 2009 le réseau Bitcoin, dont le registre n'a jamais été falsifié par une attaque. Des banques, des logisticiens et des administrations la testent ou l'utilisent pour garantir l'intégrité de leurs registres — l'Estonie, par exemple, pour certains registres publics.

Elle a fait ses preuves. Elle n'est pas magique pour autant : bien conçue et bien auditée, elle est robuste.

Réponse à l'objection classique

« Mais c'est compliqué, la blockchain ! »

Non. Utiliser la blockchain est simple. Comprendre comment elle fonctionne, c'est un peu plus technique. Mais devinez quoi : vous n'avez pas besoin de comprendre un moteur de voiture pour conduire. Vous n'avez pas besoin de comprendre les algorithmes bancaires pour faire un virement. Et vous n'aurez pas besoin de comprendre la blockchain pour voter.

Reste une question légitime, après l'échec des machines à voter : pourquoi la blockchain ne reproduirait-elle pas la même opacité logicielle ? La réponse tient en un mot, que le chapitre 4 va détailler : l'ouverture. Une blockchain bien conçue pour le vote n'est pas une boîte noire qu'il faut croire sur parole — c'est un registre public que n'importe qui peut consulter et vérifier. C'est toute la différence.

8. Fin de l'urne, début de la vérification

L'urne traditionnelle a eu une belle vie. Elle a accompagné plus d'un siècle de démocratie. Elle a permis des révolutions, des alternances, des progrès. On lui doit beaucoup.

L'évolution nécessaire

Mais aujourd'hui, elle est obsolète. Comme le minitel face à Internet. Comme le fax face à l'email. Comme le chèque face au virement instantané.

Ce n'est pas une trahison. C'est une évolution.

La transition historique

L'urne est morte. Pas parce qu'elle était mauvaise. Mais parce que nous pouvons faire mieux.

TRANSITION VERS LE CHAPITRE 3

Mais avant d'expliquer comment fonctionne la blockchain, une question s'impose : pourquoi ne pas simplement réformer le système actuel ? C'est l'objet du prochain chapitre.

Puis, au chapitre 4, nous vous expliquerons tout : avec des mots simples, des schémas clairs, des exemples concrets. Parce que si la Démocratie 3.0 doit arriver, il faut que tout le monde comprenne. Pas juste les geeks. Pas juste les politiques. Tout le monde.

Vous venez de voir l'ampleur du problème. Découvrons maintenant la solution qui va tout changer.

Le futur du vote commence maintenant.

CHAPITRE 3

L'IMPASSE TOTALE

« Quand toutes les portes sont fermées, il faut construire sa propre sortie. »

Introduction : quand toutes les voies sont bloquées

Nous avons posé le diagnostic (Chapitre 1) : le système électoral repose sur une foi aveugle que plus personne n'accorde.

Nous avons identifié les failles (Chapitre 2) : impossibilité de vérifier, erreurs humaines, fraude possible, obsolescence technologique.

La question logique se pose alors : pourquoi ne réforme-t-on pas le système ?

La réponse est brutale : parce que toutes les tentatives de réforme ont échoué. Pas par manque de volonté citoyenne. Pas par manque d'idées. Par résistance structurelle du système lui-même.

Ce chapitre démontre pourquoi l'impasse est totale — et pourquoi la voie la plus réaliste consiste à construire un système parallèle plutôt qu'à attendre que l'ancien se réforme de l'intérieur.

1. L'illusion de la réforme de l'intérieur

Le piège de la délégation

Depuis des décennies, face aux crises de confiance successives, les citoyens ont demandé des réformes : plus de transparence, des audits indépendants, une modernisation du vote, un contrôle citoyen renforcé.

Mais qui décide de ces réformes ? L'État. Les élus. Les bénéficiaires du système actuel.

C'est comme demander à une banque soupçonnée de fraude de s'auditer elle-même, ou à un arbitre accusé de partialité de réviser ses propres décisions. Conflit d'intérêts structurel.

Pourquoi l'État ne se réforme presque jamais en profondeur

RAISON N°1 — L'intérêt personnel. Les élus en place ont été élus par le système actuel. Le réformer en profondeur reviendrait à admettre que leur propre légitimité repose sur une base fragile. Aucun pouvoir ne scie la branche sur laquelle il est assis.

RAISON N°2 — La peur de l'inconnu. Les hauts fonctionnaires et les décideurs politiques sont formés dans une culture de contrôle vertical. L'idée d'un système transparent, auditable par le citoyen, leur paraît dangereuse et ingérable. « Et si les citoyens trouvent des erreurs ? Et si la transparence révèle des dysfonctionnements ? Et si nous perdons le contrôle du récit ? » La transparence est perçue comme une menace, pas comme une solution.

RAISON N°3 — L'inertie administrative. Changer le système électoral impliquerait de former des dizaines de milliers de bureaux de vote, de modifier le code électoral, de convaincre le Conseil constitutionnel, de gérer la transition technologique et d'affronter les résistances syndicales. C'est un chantier titanesque. Face à cette montagne, les gouvernements successifs choisissent la facilité de l'immobilisme : quelques ajustements cosmétiques, et on continue comme avant.

Les réformes cosmétiques des vingt dernières années

Année	Réforme proposée	Résultat	Impact sur la confiance
1969	Loi autorisant les machines à voter	Usage resté marginal pendant des décennies	Nul
2007-2008	Machines à voter électroniques	Moratoire après le bilan de 2007 ; plus aucune nouvelle commune équipée	Négatif
2014	Rapport sénatorial sur le vote électronique (Anziani-Lefèvre)	Risques pour le secret et la sincérité du vote soulignés ; pas de réforme structurelle	Nul
2017	Vote par Internet des Français de l'étranger (législatives)	Suspendu en mars 2017 sur avis négatif de l'ANSSI : risque de cyberattaque, sans piratage avéré	Négatif

Sources : réponse du ministère de l'Intérieur à la question écrite n° 03181 du sénateur Bernard Bonne (JO Sénat, 26 décembre 2019) ; arrêté du

ministre des Affaires étrangères publié au Journal officiel le 24 mars 2017, pris après l'avis de l'ANSSI du 16 mars 2017.

Le schéma est toujours le même : une crise de confiance émerge, une promesse de réforme est faite, une commission ou une loi cosmétique est votée, rien ne change structurellement, et l'on revient à la case départ.

Le verrouillage constitutionnel

En France, toute réforme profonde du système électoral se heurte à un principe constitutionnel. L'article 3 de la Constitution dispose que le suffrage « est toujours universel, égal et secret ». Le secret du vote n'est donc pas une simple tradition : c'est une exigence de la Constitution, que le Code électoral et la jurisprudence ont précisée au fil des décennies.

Toute innovation qui toucherait à ce secret est donc examinée avec une extrême prudence. La CNIL, par exemple, exige dans sa recommandation de 2019 sur le vote par Internet une séparation stricte entre l'identité des électeurs et le contenu de leurs votes. Traduction concrète pour l'électeur : dans le système officiel, vous ne pouvez pas vérifier votre propre vote a posteriori. C'est un principe solidement ancré, qu'une réforme technique ordinaire ne suffit pas à déplacer.

Pour aller plus loin, il faudrait sans doute une révision constitutionnelle : un texte adopté dans les mêmes termes par l'Assemblée nationale et le Sénat, puis approuvé par référendum ou, s'il est présenté par le gouvernement, par le Parlement réuni en Congrès à la majorité des trois cinquièmes (article 89 de la Constitution). Or la probabilité que les élus en exercice votent pour un système qui les placerait sous surveillance citoyenne directe est très faible.

2. L'échec de la confrontation stérile

Quand la colère ne suffit pas

Face à l'impossibilité de réformer de l'intérieur, les citoyens ont tenté la confrontation : manifestations, grèves, occupations, pétitions. Résultat : un échec quasi total.

Le cas emblématique : les Gilets Jaunes (2018-2019)

Le mouvement des Gilets Jaunes est l'exemple le plus complet de la confrontation stérile.

Contexte. En novembre 2018, une hausse des taxes sur les carburants déclenche une mobilisation massive — près de 283 000 manifestants le 17 novembre 2018 selon le ministère de l'Intérieur —, en particulier dans la France périphérique.

Revendications initiales : baisse des taxes, pouvoir d'achat, justice fiscale.

Revendications profondes, apparues en cours de mouvement : un référendum d'initiative citoyenne (RIC), la transparence sur l'usage de l'argent public, la fin des privilèges perçus des élites, un contrôle citoyen sur les décisions politiques. C'était, à ce moment-là, un mouvement qui touchait aux racines du système.

La réponse de l'État a suivi un cycle en quatre phases.

Phase 1 — Ignorer : « C'est marginal, ça va passer. »

Phase 2 — Réprimer : le maintien de l'ordre a fait un usage massif de LBD, de grenades de désencerclement et de techniques d'encerclement (nasses). L'usage du LBD a été vivement critiqué, jusqu'au Conseil de l'Europe, qui a appelé en février 2019 à en suspendre l'usage. Les bilans varient selon les sources et les méthodes de comptage, mais on retient généralement une dizaine de morts en marge du mouvement, pour la plupart dans des accidents de la route aux abords des blocages, plusieurs milliers de blessés dont une part importante de blessés graves, et plusieurs milliers d'interpellations sur toute la durée du mouvement [*estimations, bilans contestés selon les sources — décomptes policiers, journalistiques et associatifs divergents*]. Quel que soit le chiffre exact retenu, l'ampleur de la réponse répressive a été largement documentée et critiquée.

Phase 3 — Négocier : le Grand Débat National (janvier-mars 2019) organise des « consultations citoyennes » à l'initiative de l'exécutif.

Phase 4 — Récupérer : des mesures cosmétiques sont annoncées — 100 euros de prime d'activité, défiscalisation des heures supplémentaires, annulation de la hausse de CSG pour certains retraités. Sur les revendications de fond — RIC, transparence, contrôle citoyen —, rien. Zéro. Nada.

Bilan, plusieurs années après

Objectif	Résultat des années suivantes	Impact
RIC	Jamais mis en place	Échec total
Transparence des budgets publics	Aucun progrès notable	Échec total
Contrôle citoyen	Aucune réforme structurelle	Échec total
Confiance dans les institutions	Toujours très faible	Aggravation
Participation électorale	Abstention record aux municipales de 2020 et aux régionales de	Aggravation

	2021	
--	------	--

Le mouvement des Gilets Jaunes s'est progressivement éteint. L'abstention a battu des records aux scrutins suivants (municipales de 2020, régionales de 2021). La défiance ne s'est jamais résorbée. Les réformes structurelles réclamées au plus fort du mouvement n'ont jamais eu lieu.

Racines contre fruits : l'erreur stratégique

Il faut ici comprendre une distinction simple. Imaginez un arbre dont les fruits sont pourris. Vous pouvez passer votre vie à arracher chaque fruit malade : l'arbre continuera à en produire. Ou vous pouvez vous attaquer aux racines : l'arbre meurt, et les fruits pourris avec lui.

Les Gilets Jaunes ont, pour l'essentiel, combattu les fruits du système — les taxes, une loi, une décision précise — plutôt que ses racines : l'opacité, le monopole du pouvoir, l'impossibilité de vérifier. « Baissez la taxe carbone », « augmentez le SMIC », « démissionnez » : ce sont des fruits. « Donnez-nous l'accès aux comptes publics », « laissez-nous auditer les budgets », « prouvez-nous que nos votes comptent » : ce sont des racines, et elles ont été beaucoup moins portées, beaucoup moins tenues dans la durée.

Le piège est là : le système peut céder sur les fruits, quitte à lâcher quelques milliards d'euros ou quelques mesures symboliques. Il ne cédera pratiquement jamais sur les racines, parce que les racines, c'est son pouvoir. Les Gilets Jaunes ont mobilisé des centaines de milliers de personnes, des mois d'énergie citoyenne, des milliers d'heures de manifestations et un capital de sympathie médiatique réel — largement absorbés par une confrontation frontale avec un système qui, par construction, ne pouvait pas céder sur l'essentiel.

C'est le drame de nombreux mouvements sociaux contemporains : ils se battent *contre* le système, quand la seule stratégie qui affaiblit durablement un monopole consiste à construire *à côté* de lui.

3. L'impuissance de la contestation juridique

Quand la loi protège l'opaque

Troisième voie tentée par les citoyens : la contestation juridique. « Si le politique refuse de changer, allons devant les tribunaux. » Résultat : une impasse quasi totale.

Le fardeau de la preuve impossible

Pour contester une élection devant le juge administratif, il faut prouver l'irrégularité. Or comment prouver une fraude électorale quand on n'a accès à aucune des données qui permettraient de la démontrer ?

Le scénario est souvent le même : un citoyen soupçonne une anomalie dans son bureau de vote. Pour des élections municipales, il ne dispose que de cinq jours après le scrutin pour saisir le tribunal administratif (article R. 119 du Code électoral). Le recours est gratuit et l'avocat n'est pas obligatoire, mais c'est à lui d'apporter des griefs précis et des éléments de preuve. Or, à ce stade, les bulletins valables ont déjà été détruits, et il ne dispose que des procès-verbaux et des listes d'émargement. Sans éléments précis, sa requête sera rejetée.

C'est un cercle vicieux : pour prouver qu'il y a fraude, il faut avoir accès aux données ; pour avoir accès aux données, il faut déjà avoir prouvé qu'il y a fraude. Structurellement, c'est presque impossible à franchir seul.

L'asymétrie des moyens

Même lorsqu'un citoyen parvient à constituer un dossier, il se heurte à une asymétrie de moyens considérable.

Le citoyen	L'État
Peut agir sans avocat, mais doit souvent en payer un pour bâtir un dossier solide (plusieurs milliers d'euros)	Dispose de services juridiques financés par l'impôt
N'a aucun accès direct aux données du scrutin	A un accès total à ses propres données
Doit apprendre à se battre contre la machine administrative	Maîtrise parfaitement les procédures et leurs délais

C'est une configuration David contre Goliath. Et dans la réalité des contentieux électoraux, David perd le plus souvent.

Un exemple illustratif

[Exemple illustratif, composite — ce scénario n'est pas le compte rendu d'une affaire précise mais une reconstitution représentative du type de contentieux électoral qui se répète, sous des formes voisines, dans de nombreuses communes françaises.]

Lors d'élections municipales, un candidat battu de peu conteste les résultats d'un bureau ou d'un secteur de vote. Les irrégularités invoquées sont classiques du genre : bourrage d'urne présumé, procurations suspectes, écarts de comptage entre le nombre d'émargements et le nombre de bulletins dépouillés. Le candidat saisit le tribunal administratif. La procédure s'étale sur plusieurs mois, parfois plus d'un an. Les frais d'avocats et d'expertise se chiffrent en milliers d'euros, à la charge du requérant. Au terme du délai, le tribunal rejette la requête : « preuves insuffisantes ». Les irrégularités étaient-elles réelles ? Personne ne le saura jamais, faute d'accès aux données brutes. Le candidat a-t-il les moyens de faire appel ? Rarement : l'argent déjà englouti dissuade la plupart de

continuer. C'est ce schéma-là, documenté à de multiples reprises dans le contentieux électoral français, qui illustre le mieux l'asymétrie décrite plus haut — indépendamment de l'identité de tel ou tel candidat ou de telle ou telle commune.

L'impossible audit citoyen

Certains citoyens tentent d'obtenir les documents du scrutin. La loi leur en ouvre une partie : les listes d'émargement peuvent être consultées par tout électeur à la préfecture pendant les dix jours qui suivent l'élection (article L. 68 du Code électoral), et les procès-verbaux sont communicables. Mais ces documents ne disent rien du contenu des bulletins, détruits le soir même du dépouillement. Ils permettent de vérifier qui a signé, pas ce qui a été compté. Pour un audit citoyen sérieux, c'est extrêmement limité.

Conclusion de cette section : le système se protège juridiquement. Toutes les voies légales de contestation existent en théorie. Dans la pratique, elles sont presque toutes hors de portée d'un citoyen isolé.

4. Le piège de l'apathie

Quand l'impuissance devient résignation

Face à l'échec des voies traditionnelles — réforme, confrontation, justice —, une partie des citoyens bascule dans l'apathie.

Le raisonnement de la résignation tient en quelques phrases : « J'ai voté pendant trente ans, rien n'a changé. » « J'ai manifesté, on m'a gazé. » « J'ai signé des pétitions, elles dorment dans un tiroir. » « À quoi bon ? »

C'est Martine, 68 ans, dont nous avons fait la connaissance au Chapitre 1 : « J'ai voté toute ma vie. Mais en 2022, pour la première fois, je suis restée chez moi. Parce que je ne crois plus que ça change quoi que ce soit. »

L'apathie, pire victoire du système

L'apathie est, pour un système qui vit de l'absence de contrôle, sa victoire la plus silencieuse — parce qu'elle transforme la colère en résignation, la revendication en silence, l'action en passivité. Un citoyen en colère est dangereux pour le système. Un citoyen résigné est inoffensif.

C'est presque, structurellement, ce que le système finit par obtenir : promettre la réforme pour calmer la colère, ne rien changer sur le fond pour protéger le monopole, attendre que la colère se transforme en lassitude. Une victoire par épuisement.

Les chiffres de l'apathie

Nous les avons vus au Chapitre 1 : 28 % d'abstention au second tour de la présidentielle de 2022, 52,5 % au premier tour des législatives de 2022, et plus d'un jeune de 18-24 ans sur deux absent des urnes à la plupart des scrutins. Ce ne sont pas des chiffres de désintérêt politique. Ce sont des chiffres de capitulation. Une génération entière a compris que le système est verrouillé, et une partie a choisi de s'en retirer — pas par paresse, par lucidité.

Cette même lucidité est ce qui, un peu plus loin dans ce chapitre, ouvre une autre possibilité : si aucune des voies classiques ne fonctionne, la question n'est plus « comment convaincre le système », mais « comment le rendre secondaire ».

5. Pourquoi toutes ces stratégies échouent

Le diagnostic

Stratégie	Résultat	Raison de l'échec
Réforme de l'intérieur	Bloquée	Conflit d'intérêts structurel
Confrontation directe	Stérile	Combat les fruits, pas les racines
Contestation juridique	Impuissante	Asymétrie des moyens
Apathie	Capitulation	Victoire silencieuse du système

Ces quatre stratégies échouent pour la même raison profonde : toutes demandent, d'une manière ou d'une autre, au système de se réformer lui-même — en changeant ses propres règles, en cédant sous la pression, ou en validant les preuves qui le mettraient en cause.

Une objection légitime : et les autres voies ?

Un lecteur attentif objectera, à raison, que ces quatre voies ne sont pas les seules envisageables. Une convention citoyenne tirée au sort et dotée d'un pouvoir constituant, un mouvement politique entièrement nouveau, ou la constitutionnalisation du référendum d'initiative citoyenne sont des pistes sérieuses, régulièrement proposées par des chercheurs et des acteurs de terrain.

Elles méritent d'être prises au sérieux — et elles butent, chacune à sa manière, sur le même obstacle que les quatre voies précédentes. Une convention citoyenne ne peut produire que des recommandations : sa mise en œuvre reste entièrement entre les mains des institutions qu'elle est censée corriger, et l'expérience récente montre à quel point ce filtre final peut vider une proposition de sa substance. Un nouveau parti doit, pour peser, se plier aux règles électorales du système qu'il conteste, et le temps

qu'il lui faut pour y parvenir — des années, parfois des décennies — laisse au monopole toute latitude pour l'absorber ou l'épuiser. Quant à la constitutionnalisation du RIC, elle suppose exactement la révision constitutionnelle décrite plus haut dans ce chapitre : un vote des trois cinquièmes du Parlement, ou un référendum, décidés par les élus mêmes qui n'ont aucun intérêt à s'y soumettre. Ces voies ne sont donc pas fausses. Elles sont, comme les quatre précédentes, suspendues à la bonne volonté du système qu'elles cherchent à changer — ce qui est précisément le nœud du problème que ce chapitre cherche à démontrer.

Une loi que l'histoire vérifie souvent

Un monopole cède rarement son pouvoir de son plein gré ; il faut le plus souvent qu'une force extérieure le rende obsolète ou intenable.

Monopole	Époque	Fin	Comment
Monarchie absolue en France	XVIIIe siècle	1789	Renversée de l'extérieur
Esclavage (dans l'Empire colonial français)	XIXe siècle	1848	Aboli sous la pression du mouvement abolitionniste
Monopoles historiques des télécommunications	XXe siècle	Années 1990	Ouverts à la concurrence (1998 en France), puis bousculés par Internet

Cette régularité historique n'est pas une garantie mathématique, mais elle a valeur d'avertissement : le monopole institutionnel sur l'organisation et la vérification du vote a peu de chances d'être réformé de l'intérieur par l'État qui le détient. Il a davantage de chances d'être rendu obsolète par un système parallèle de vérification, construit à côté de lui.

6. La seule issue crédible : construire à côté

Changer de paradigme

Toutes les stratégies précédentes partent du même postulat : il faut convaincre le système de changer. Ce chapitre propose d'inverser ce postulat. Il ne s'agit pas de convaincre, mais de construire un système alternatif qui rend l'ancien obsolète — sans attendre son autorisation.

La leçon de la disruption technologique

Ancien monopole	Disrupteur	Stratégie
Taxis	Uber	Ne pas demander la permission au secteur en place
Hôtellerie traditionnelle	Airbnb	Contourner le monopole hôtelier
Banques	Bitcoin	Prouver qu'on peut transférer de la valeur sans elles
Vérification électorale d'État	ShadowVote	Créer une vérification parallèle

Cette comparaison a une limite qu'il faut assumer honnêtement : Uber et Airbnb ont fini, dans de nombreux pays, par être largement régulés, encadrés, parfois interdits localement. Rien ne garantit qu'un État ne cherche pas, un jour, à faire de même avec un système de vérification citoyenne. La différence est que le ShadowVote, tel qu'il est conçu dans ce livre, ne prétend remplacer aucun scrutin officiel : il ne fait que rendre publique et vérifiable une donnée que chaque citoyen a le droit moral de connaître — combien de personnes ont, comme lui, exprimé tel choix. Interdire un miroir citoyen non contraignant est un geste politiquement bien plus coûteux qu'interdire un concurrent commercial. Nous y reviendrons en détail dans la Partie II.

Pourquoi cette stratégie a des chances de fonctionner

Raison n°1 — elle ne dépend pas du système. Le ShadowVote ne demande aucune autorisation, ne nécessite aucune loi nouvelle, ne requiert aucune validation du Conseil constitutionnel. C'est un vote citoyen parallèle et non contraignant, qui devra bien sûr respecter le droit existant : ne publier aucun résultat avant la fermeture du dernier bureau de vote (article L. 52-2 du Code électoral), et traiter les opinions politiques — des données sensibles au sens de l'article 9 du RGPD — avec le consentement explicite des participants. L'État aurait du mal à l'interdire sans donner l'impression que la vérification le menace.

Raison n°2 — elle inverse la charge de la preuve. Aujourd'hui, c'est au citoyen de prouver qu'il y a fraude. Avec un système de vérification parallèle actif et massivement utilisé, c'est à l'État qu'il reviendrait d'expliquer un écart significatif entre ses résultats et ceux, transparents et vérifiables, du miroir citoyen. Le fardeau de la preuve se déplace.

Raison n°3 — elle crée une pression progressive. Quand 1 % des électeurs utilisent le ShadowVote, la pression commence à peine. Quand 5 % l'utilisent, elle devient difficile à ignorer. Quand 10 % l'utilisent, le système est contraint de réagir : soit les résultats convergent, et la confiance revient ; soit ils divergent, et la question de l'opacité devient publique et difficile à esquiver. Dans les deux cas, le débat avance.

Conclusion : l'impasse est réelle, mais une porte reste ouverte

Nous avons parcouru les principales voies traditionnelles. La réforme de l'intérieur : bloquée par le conflit d'intérêts. La confrontation directe : épuisée dans des combats souvent stériles. La contestation juridique : écrasée par l'asymétrie des moyens. L'apathie : une capitulation silencieuse. Les alternatives institutionnelles plus récentes — convention citoyenne, nouveau parti, RIC constitutionnalisé — restent, elles aussi, suspendues au bon vouloir du système qu'elles voudraient réformer.

Une porte reste néanmoins ouverte : celle qui ne demande la permission à personne, celle du code.

Le ShadowVote n'est pas une réforme du système. C'est un système parallèle, conçu pour rendre l'ancien obsolète à force de transparence. Plutôt que de supplier l'État de nous donner accès à la vérité des urnes, nous pouvons la construire nous-mêmes. Plutôt que de mendier le droit de vérifier, nous pouvons vérifier.

L'impasse est réelle. La solution, elle, est à notre portée.

TRANSITION VERS LA PARTIE II

Dans la Partie II, nous allons découvrir comment fonctionne cette solution. Nous allons comprendre la blockchain sans jargon technique. Nous allons voir, en détail, l'architecture du ShadowVote. Nous allons répondre à toutes les objections légitimes qu'un lecteur exigeant peut déjà se poser.

Et vous allez réaliser une chose : ce n'est pas une utopie. C'est faisable, maintenant, avec la technologie qui existe déjà.

Vous venez de voir l'ampleur du problème. Découvrons maintenant la solution qui va tout changer.

CHAPITRE 4

LA BLOCKCHAIN POUR TOUS

« La meilleure technologie est celle qu'on ne voit pas. »

Introduction : le mot qui fait peur

Blockchain.

Voilà. Le mot est lâché.

Pour beaucoup d'entre vous, ce mot évoque :

- Des geeks incompréhensibles
- Des cryptomonnaies louches
- Des arnaques au Bitcoin
- Un jargon technique impénétrable

Et vous avez raison d'être méfiant.

Le problème de réputation

Le monde de la blockchain a été pollué par :

- Des escrocs qui ont monté des pyramides de Ponzi
- Des spéculateurs qui ont créé des bulles financières
- Des « experts » qui parlent pour ne rien dire
- Des projets fumeux qui promettent la lune

Mais.

Au milieu de ce bruit, il y a une technologie sérieuse qui, utilisée correctement, peut répondre au problème posé dans les chapitres précédents : comment redonner à un vote la confiance, la preuve et la transparence qui lui manquent.

L'objectif de ce chapitre

Ce chapitre a un seul objectif : vous faire comprendre la blockchain.

- Sans jargon
- Sans formules mathématiques
- Sans vous demander de devenir ingénieur
- Juste avec des images simples

À la fin de ce chapitre, vous comprendrez :

- Ce qu'est vraiment une blockchain
- Pourquoi elle est si difficile à falsifier

- Comment elle peut aider à réparer le vote
- Pourquoi c'est différent du vote électronique classique

Prêt ?

1. La blockchain expliquée à votre grand-mère

Analogie 1 : le Grand Livre du Village

Imaginez un village de 1 000 habitants.

Dans ce village, il n'y a pas de banque. Les habitants ont trouvé un autre système pour gérer leurs échanges d'argent : le Grand Livre du Village.

Comment ça marche ?

ÉTAPE 1 : LE LIVRE EXISTE

Il y a un énorme registre, posé sur la place du village. Tout le monde peut le consulter. Personne ne peut l'arracher ou le cacher.

Dans ce livre, chaque transaction est notée :

- « Lundi 10h : Marie donne 50€ à Paul »
- « Lundi 14h : Paul donne 20€ à Sophie »
- « Mardi 9h : Sophie donne 30€ à Jean »

Tout est écrit. Rien ne disparaît.

ÉTAPE 2 : TOUT LE MONDE SURVEILLE

Quand Marie veut donner 50€ à Paul, elle ne lui donne pas de billets. Elle écrit dans le Grand Livre : « Marie → Paul : 50€ ».

Mais pour que cette transaction soit valide, il faut que 10 habitants du village (choisis au hasard) vérifient que Marie a bien 50€ disponibles.

- Ils consultent le livre.
- Ils vérifient l'historique des transactions de Marie.
- Si Marie a 50€ → les 10 habitants signent la transaction.
- Si Marie n'a que 20€ → la transaction est refusée.

La validation est collective.

ÉTAPE 3 : LE LIVRE EST INVOLABLE

Imaginons que Marie soit malhonnête. Elle veut effacer une transaction où elle a donné 50€ à Paul, pour récupérer son argent.

Elle attend la nuit. Elle va sur la place. Elle arrache la page.

Problème : le lendemain matin, les 1 000 habitants du village ont tous une copie du livre chez eux. Ils comparent. Ils voient que la page manque dans le livre de la place. Ils la recollent.

Marie ne peut pas effacer la transaction, car elle devrait effacer 1 000 copies du livre en même temps. Impossible.

ÉTAPE 4 : LE LIVRE GRANDIT, BLOC PAR BLOC

Chaque jour, une nouvelle page est ajoutée au livre. Mais cette page est scellée : elle est attachée à la page précédente par un code secret — un « sceau de cire » numérique.

Si quelqu'un tente de modifier une page du passé, le sceau se brise, et tout le monde voit que le livre a été trafiqué.

Le passé est figé. Pour toujours.

La correspondance parfaite

Voilà. Vous venez de comprendre la blockchain.

Grand Livre du Village	Blockchain
Le registre sur la place	La blockchain
Chaque transaction	Un enregistrement
Chaque page	Un « bloc »
Le sceau entre les pages	Le « hash cryptographique »
Les 1 000 copies	Les « nœuds décentralisés »
Les 10 habitants validateurs	Le « consensus »

C'est aussi simple que ça. Retenez bien ce tableau : dans tout le reste du chapitre, chaque fois qu'un mot technique apparaîtra, il vous suffira de repenser à sa case de gauche.

Analogie 2 : le match de foot sans arbitre corrompu

Deuxième image pour comprendre pourquoi la blockchain est si difficile à corrompre.

Imaginez un match de football.

Système classique (centralisé)

Il y a un arbitre. C'est lui qui compte les buts, siffle les fautes, valide le score.

Problème : si l'arbitre est corrompu (acheté par une équipe), il peut ne pas siffler un penalty évident, valider un but hors-jeu, falsifier le score final. Et vous, spectateur, vous ne pouvez rien faire. Vous criez, vous contestez, mais c'est l'arbitre qui décide. Son cahier de score fait foi.

Système blockchain (décentralisé)

Il n'y a pas d'arbitre unique. Il y a 10 000 spectateurs dans le stade. Chacun a un cahier. Chacun note les buts en temps réel.

À la fin du match, on compare les 10 000 cahiers.

- Si 9 999 cahiers disent « 3-2 » et qu'un seul dit « 5-0 » → le menteur est démasqué.
- Si 5 000 cahiers disent « 3-2 » et 5 000 disent « 2-3 » → on revoit la vidéo (une preuve extérieure tranche).

Le score final est celui validé par la majorité.

Pourquoi tricher devient impossible

Maintenant, imaginez qu'une équipe veuille tricher. Elle devrait acheter 5 001 spectateurs — la majorité. Coût : des millions d'euros. Risque : être immédiatement démasquée, car les 4 999 autres spectateurs dénoncent la fraude.

Conclusion : tricher devient plus coûteux que jouer honnêtement.

Le principe fondamental

Voilà pourquoi la blockchain est si difficile à corrompre. Ce n'est pas parce que les gens sont vertueux. C'est parce que la fraude coûte plus cher que l'honnêteté.

2. Blockchain vs vote électronique classique

Pourquoi les machines à voter ont échoué

Dans le Chapitre 2, nous avons vu que les machines à voter électroniques (utilisées surtout au milieu des années 2000, puis gelées par un moratoire en 2008) ont été un échec en France. Rappel des problèmes :

- Opacité totale (code source fermé)
- Vulnérabilité informatique (piratage facilité)
- Absence de preuve papier (aucune trace physique)
- Centralisation (une seule machine = un seul point de défaillance)

La blockchain répond à ces quatre problèmes — pas en les faisant disparaître par magie, mais en changeant l'architecture du système.

Problème 1 : l'opacité → Solution : le code ouvert

Machine à voter classique	Blockchain (ShadowVote)
✗ Code source secret (propriété de l'entreprise)	✓ Code source ouvert et public

✗ Vous ne savez pas comment ça marche	✓ N'importe quel développeur peut le vérifier
✗ Confiance dans le fabricant	✓ Confiance dans un code que tout le monde peut lire

Résultat : transparence totale.

Problème 2 : la vulnérabilité → Solution : la copie multiple (« décentralisation »)

Machine à voter classique	Blockchain (ShadowVote)
✗ Une seule machine par bureau de vote	✓ Des milliers de copies identiques du registre, réparties sur des ordinateurs différents
✗ Si elle est piratée → tout le bureau est compromis	✓ Pour falsifier le résultat, il faudrait pirater la majorité de ces copies en même temps
✗ Un point unique de défaillance	✓ Un objectif quasiment inatteignable en pratique

Résultat : une résilience beaucoup plus grande.

Problème 3 : l'absence de trace → Solution : le registre permanent

Machine à voter classique	Blockchain (ShadowVote)
✗ Vote stocké dans la mémoire d'une machine	✓ Chaque vote enregistré de façon permanente
✗ En cas de panne → tout est perdu	✓ Tant qu'une seule copie survit, le registre entier survit
✗ Aucune trace physique	✓ Une trace numérique indestructible

Résultat : une mémoire durable du scrutin.

Problème 4 : la centralisation → Solution : le réseau réparti

Machine à voter classique	Blockchain (ShadowVote)
✗ Résultats stockés dans la mémoire de chaque machine, invérifiables de l'extérieur	✓ Résultats répliqués sur des milliers de machines
✗ Si une machine est trafiquée → les votes de tout le bureau sont compromis	✓ Aucun serveur central à faire tomber
✗ Un gestionnaire unique contrôle l'ensemble	✓ Aucun acteur unique ne contrôle la blockchain

Résultat : un système beaucoup plus difficile à censurer ou à saboter d'un seul coup.

Tableau comparatif final

Critère	Machine à voter	Blockchain (ShadowVote)
Transparence	✗ Code secret	✓ Code ouvert
Sécurité	✗ Point unique de défaillance	✓ Réparti sur de nombreuses machines
Traçabilité	✗ Aucune trace	✓ Registre permanent
Auditabilité	✗ Impossible	✓ N'importe qui peut vérifier le code
Coût de la fraude	Faible (pirater une machine)	Élevé (il faut compromettre la majorité du réseau)

La blockchain n'est pas « du vote électronique ». C'est une technologie fondamentalement différente dans sa manière de stocker et de protéger l'information.

3. Comment ça marche vraiment (avec les mêmes images qu'avant)

Les 5 briques de base

Vous connaissez déjà le Grand Livre du Village et le stade aux 10 000 cahiers. Bonne nouvelle : la blockchain, techniquement, ce sont exactement les mêmes cinq idées, avec des noms un peu plus savants. Voyons-les une par une, chaque nom technique accompagné aussitôt de son image simple.

Brique 1 : le registre public — c'est le Grand Livre

La blockchain est un registre, un grand cahier où toutes les transactions (ou tous les votes) sont notés.

- Public : n'importe qui peut le consulter, comme le livre posé sur la place du village.
- Permanent : une fois écrit, impossible à effacer, comme les pages du Grand Livre.
- Chronologique : tout est daté et ordonné, jour après jour.

Brique 2 : les blocs — ce sont les pages du livre

Le registre n'est pas un long fichier unique. Il est découpé en blocs, exactement comme le Grand Livre est découpé en pages.

Chaque bloc contient un paquet de transactions (par exemple 1 000 votes), une date et une heure, et un lien vers le bloc précédent — le fameux sceau de cire numérique.

Pourquoi des blocs ? Pour rendre la fraude visible immédiatement. Si vous modifiez un bloc du passé — par exemple un vote enregistré il y a trois mois — le sceau qui le relie au reste du livre se brise, et tous les blocs suivants deviennent suspects. C'est comme un château de cartes : touchez une carte tout en bas, et l'édifice entier vacille au-dessus.

Brique 3 : le hash — c'est le sceau de cire numérique

Le mot technique « hash » désigne exactement le sceau de cire dont on parle depuis le début. Rien de plus mystérieux que ça.

Concrètement : c'est une empreinte digitale numérique. Imaginez que vous preniez un livre entier de 500 pages et que vous le passiez dans une machine qui en tire un code unique, une suite de chiffres et de lettres qui ressemble à ceci :

```
`3a5f7c9d2e1b8f4a6c3e9d7b2f1a5c8e9d2b4f7a3c6e1d9b5f2a8c4e7d3b6f1a9`
```

Ce code est unique au texte exact qu'on lui a donné. Changez un seul mot dans le livre, et le code change entièrement — comme une empreinte digitale qui ne ressemble à aucune autre. C'est ça, un hash : le sceau de cire, mais calculé par un ordinateur plutôt que pressé dans la cire.

Appliqué à la blockchain : chaque page (chaque bloc) a son propre sceau, et chaque page porte aussi imprimé le sceau de la page précédente. Résultat : si vous modifiez la page N, son sceau change — mais la page N+1 garde en mémoire l'ancien sceau. La différence saute aux yeux de quiconque compare. La fraude se voit.

Brique 4 : les nœuds — ce sont les 1 000 copies chez les villageois

La blockchain n'existe pas sur un seul ordinateur. Elle existe sur des milliers d'ordinateurs en même temps, exactement comme les 1 000 exemplaires du Grand Livre que chaque villageois garde chez lui. Chaque ordinateur qui garde une copie s'appelle un « nœud » — un mot savant pour dire, tout simplement, « un villageois qui a sa copie du livre ».

Si un nœud est piraté ou détruit, tous les autres conservent le registre intact.

Une autre image, celle du testament

Imaginez que vous écrivez votre testament.

- Version centralisée : vous le confiez à un notaire unique. Si son bureau brûle, votre testament disparaît.
- Version décentralisée : vous en donnez une copie à 10 000 notaires. Pour le détruire, il faudrait brûler 10 000 bureaux en même temps. Impossible.

C'est exactement le principe des nœuds : plus il y a de copies indépendantes, plus le registre est difficile à faire disparaître.

Brique 5 : le consensus — c'est le vote des 10 habitants, ou celui des 10 000 spectateurs

Quand un nouveau vote arrive, qui décide s'il est valide ? Pas un ordinateur central, pas une autorité unique, mais un accord collectif entre les nœuds — c'est exactement ce que faisaient les 10 habitants du village en vérifiant le compte de Marie, ou les 10 000 spectateurs en comparant leurs cahiers. Le mot technique pour cet accord collectif est « consensus » : reprenez-le comme un synonyme savant de « vote entre machines ».

Comment ça marche, concrètement ?

1. Alice vote. Son vote est transmis à un grand nombre de nœuds (les ordinateurs du réseau). 2. Chaque nœud vérifie : Alice est-elle bien inscrite sur les listes ? A-t-elle déjà voté ? Le vote est-il dans le bon format ? 3. Si la majorité des nœuds valide le vote, il est ajouté au bloc. 4. Le bloc est scellé avec son hash et distribué à tous les nœuds — comme la nouvelle page du Grand Livre, recopiée chez tous les villageois le lendemain matin.

Pourquoi la majorité ?

Pour falsifier un vote, un fraudeur devrait convaincre ou contrôler la majorité des nœuds — exactement comme, dans le stade, il faudrait acheter 5 001 spectateurs sur 10 000 pour changer le score. Sur un réseau comme celui du Bitcoin, où les nœuds se comptent par dizaines de milliers dans le monde entier, les estimations économiques évoquent un coût de plusieurs milliards d'euros pour tenter une telle opération — et même à ce prix, la fraude serait vite repérée, puisque les autres nœuds continueraient de faire tourner l'ancienne version honnête du registre.

Ce chiffre concerne un réseau de la taille de Bitcoin. Le nombre de nœuds que comptera effectivement ShadowVote — et donc le coût réel d'une attaque contre lui — dépendra de son architecture précise. C'est un point que nous détaillerons au Chapitre 5 : plus le réseau de vérification est large et indépendant, plus la fraude devient coûteuse et détectable.

Retenez la conclusion, qui vaut pour tous les réseaux bien conçus : frauder doit coûter plus cher que jouer honnêtement.

4. La blockchain est-elle vraiment difficile à corrompre ?

Trois garanties, avec leurs limites

Garantie 1 : l'immutabilité

Une fois qu'un vote est enregistré dans la blockchain, le modifier sans être détecté est extrêmement difficile.

Pourquoi ? À cause du système de sceaux (Brique 3). Modifier un bloc ancien casse tous les sceaux suivants, comme retirer une carte au milieu d'un château de cartes de dix mille étages : impossible sans que tout l'édifice ne s'effondre visiblement.

Garantie 2 : la résilience

Même si l'immense majorité des serveurs disparaissait — guerre, catastrophe, attaque massive — les copies restantes conserveraient l'intégralité du registre.

Pourquoi ? Grâce à la copie multiple entre les nœuds (Brique 4). C'est comme si un tableau précieux était recopié à l'identique dans dix mille musées : le détruire partout à la fois est hors de portée.

Garantie 3 : la transparence

N'importe qui peut vérifier la blockchain, contrôler les votes, recompter les résultats.

Pourquoi ? Parce que le registre est public (Brique 1). Tout est visible, en permanence — comme un scrutin qui se déroulerait en plein air, sur une place publique, sous le regard de milliers de témoins.

Ces trois garanties sont solides, mais elles ne sont pas magiques : elles dépendent d'une mise en œuvre rigoureuse (un code bien audité, un réseau suffisamment large et indépendant). C'est un travail sérieux, pas un coup de baguette.

Mais alors, pourquoi tout le monde n'utilise pas la blockchain ?

Bonne question.

Raison 1 : la complexité technique

La blockchain est simple à comprendre — vous venez de le faire en quelques pages. Mais elle est complexe à mettre en œuvre correctement : il faut des développeurs compétents, des audits de sécurité rigoureux, une infrastructure répartie, une gouvernance claire. Ce n'est pas insurmontable, mais ça demande du travail sérieux.

Raison 2 : la résistance culturelle

Les institutions — État, banques, grandes entreprises — ont été construites sur un modèle centralisé : un responsable, une hiérarchie, un contrôle vertical. La blockchain propose l'inverse : pas de patron unique, un réseau horizontal, un contrôle collectif. C'est un changement culturel, pas seulement technique, et ceux qui tiennent les manettes du système actuel n'ont pas toujours intérêt à s'en défaire.

Raison 3 : les arnaques ont sali l'image

Les cryptomonnaies (Bitcoin, Ethereum, et bien d'autres) ont attiré des spéculateurs, des escrocs montant des pyramides de Ponzi, parfois des blanchisseurs d'argent. Résultat : le grand public associe souvent « blockchain » à « arnaque ».

La distinction cruciale

Mais. Bitcoin n'est pas la blockchain. Bitcoin est une application de la blockchain — le transfert d'argent. ShadowVote en serait une autre application — le vote.

C'est un peu comme confondre l'automobile avec les accidents de la route : la voiture a permis des drames, mais elle a aussi permis l'ambulance, le camion de pompiers et des millions de trajets sans encombre. L'outil n'est pas réductible à son pire usage. Internet a plein d'usages différents. La blockchain aussi.

5. Les objections techniques (et leurs réponses)

Objection 1 : « C'est trop compliqué pour les gens »

RÉPONSE :

Utiliser la blockchain n'est pas plus compliqué qu'utiliser une application sur votre téléphone. Vous n'avez pas besoin de comprendre comment fonctionne Internet pour envoyer un e-mail. Vous n'avez pas besoin de comprendre la cryptographie — la science des codes secrets qui protège vos échanges — pour utiliser votre carte bancaire. De même, vous n'aurez pas besoin de comprendre le hash pour voter sur ShadowVote.

L'interface serait simple : vous ouvrez l'application, vous choisissez votre candidat, vous validez, vous recevez un reçu — un code qui prouve que votre vote a bien été enregistré, comme le ticket que vous donne une carte bancaire après un paiement. Temps nécessaire : environ 30 secondes.

Objection 2 : « Les pirates vont attaquer la blockchain »

RÉPONSE :

Attaquer une blockchain bien conçue est extraordinairement difficile avec la technologie actuelle. Pour falsifier un vote, il faudrait contrôler la majorité des nœuds (revoir la Brique 5), recalculer tous les sceaux depuis le bloc frauduleux, et le faire plus vite que le reste du réseau, honnête, ne produit de nouveaux blocs. Nous l'avons vu : sur un réseau de grande taille, ce genre d'opération coûterait des sommes considérables et serait presque certainement repérée. Sur ce point précis — falsifier le registre lui-même

—, une blockchain solide est bien plus difficile à attaquer qu'une base de données centralisée.

Mais attention : les vraies failles ne sont pas là où on les attend

La blockchain elle-même est très difficile à corrompre. Mais l'interface qui vous permet d'y accéder — votre téléphone, le site internet — peut, elle, être vulnérable, exactement comme n'importe quel autre service en ligne.

Exemples de failles possibles :

- Votre téléphone est infecté par un virus (les informaticiens disent « malware », un logiciel malveillant installé à votre insu).
- Le site du ShadowVote est visé par une fausse page piège qui imite le vrai site pour vous voler votre mot de passe (les informaticiens disent « phishing », littéralement « pêche à l'hameçon »).
- Votre mot de passe est volé.

Ces risques existent aussi avec votre banque en ligne, votre boîte e-mail, votre compte des impôts. Ce n'est pas propre à la blockchain — c'est le prix de tout service numérique.

Solutions envisagées : une double vérification pour se connecter (un SMS en plus du mot de passe, ou votre empreinte digitale), des audits de sécurité réguliers, et de la pédagogie auprès des utilisateurs pour reconnaître les pièges. Aucun système n'est sûr à 100 %. Mais un système bien construit peut être rendu plus sûr, sur ces points précis, que l'urne papier ne l'est sur les siens.

Objection 3 : « L'anonymat du vote sera compromis »

RÉPONSE :

C'est LA préoccupation légitime numéro un. Comment garantir que personne ne sait pour qui vous avez voté ?

Précisons d'abord un mot important, pour être honnête avec vous : ce que la blockchain permet, ce n'est pas exactement l'« anonymat » au sens strict et juridique du terme — c'est ce qu'on appelle la pseudonymisation forte. La nuance compte, et la CNIL (l'autorité qui protège vos données personnelles) la fait clairement : un identifiant est dit « anonyme » seulement s'il est, en théorie, impossible de le relier un jour à qui que ce soit ; il est dit « pseudonyme » si ce lien existe quelque part, même verrouillé derrière des protections très solides. C'est ce second cas, plus honnête à annoncer, qui s'applique ici.

Voici comment ça marche, concrètement :

ÉTAPE 1 : VOUS CRÉEZ UNE IDENTITÉ NUMÉRIQUE

Quand vous vous inscrivez sur ShadowVote, vous ne donnez pas votre nom en clair au registre. Vous recevez un identifiant — une suite de caractères, par exemple `8f3e7a2d9c1b5e4f6a8d3c7b2e1f9a4c` — qui joue le rôle d'un pseudonyme. Cet identifiant est unique (personne d'autre ne peut l'avoir), protégé (on ne peut pas remonter à vous facilement à partir de lui seul) et vérifiable (vous seul pouvez prouver qu'il vous appartient).

ÉTAPE 2 : VOUS VOTEZ AVEC CET IDENTIFIANT

Quand vous votez, la blockchain enregistre : « L'identifiant 8f3e7a... a voté pour le Candidat X. »

Ce que tout le monde peut voir	Ce que le grand public ne peut pas voir
☒ Qu'un vote a été enregistré	☒ Qui est cette personne dans la vraie vie
☒ Que l'identifiant 8f3e7a... a voté	☒ Son nom, son prénom, son adresse

ÉTAPE 3 : VOUS SEUL POUVEZ VÉRIFIER VOTRE VOTE

Vous gardez un code secret, comme un mot de passe. Avec ce code, vous pouvez vérifier que votre vote est bien inscrit dans la blockchain, et voir pour qui vous avez voté — vous, et vous seul.

Mais vous ne pouvez PAS prouver à quelqu'un d'autre pour qui vous avez voté, même si vous le vouliez. C'est ce détail, très concret, qui protège contre l'achat de vote (« prouve-moi que tu as voté pour X, je te donne 50€ ») et contre la coercition (« si tu ne votes pas pour Y, tu es viré ») : personne d'autre que vous ne peut exhiber la preuve de votre choix.

Cette protection est réelle et solide au quotidien. Elle n'équivaut simplement pas, sur le plan juridique, à une anonymisation totale — un point sur lequel un projet comme ShadowVote devra être transparent, se soumettre à une évaluation par des juristes spécialisés en protection des données, et respecter le cadre du RGPD, tout comme il devra composer avec l'encadrement légal, aujourd'hui très strict en France, du vote électronique pour les scrutins politiques nationaux. Ce sont des chantiers pour les prochains chapitres et pour la mise en œuvre du projet — pas des détails qu'on peut balayer d'un revers de main.

Comparaison finale

Critère	Urne papier	Blockchain (ShadowVote)
Confidentialité du choix	☒ Oui	☒ Oui (pseudonymisation forte)
Vérifiable par	☒ Non	☒ Oui, par vous seul

l'électeur		
Traçable	✗ Non	✓ Oui (registre public)
Preuve de vote	✗ Aucune	✓ Un reçu numérique

ShadowVote viserait à combiner l'essentiel de l'urne — la confidentialité du choix — avec ce que le papier ne permet pas : la vérifiabilité individuelle.

Objection 4 : « Ça va coûter une fortune »

RÉPONSE :

Non. Mais il faut comparer ce qui est comparable.

Coût du système actuel (chiffres officiels)

Poste	Coût
Présidentielle et législatives de 2012 (deux scrutins, quatre tours)	432 millions €
Soit, en moyenne, par scrutin national	≈ 216 millions €
Ce que couvre ce chiffre	Propagande électorale, remboursement des dépenses de campagne, organisation matérielle (État et communes)

Source : rapport d'information d'Hervé Marseille, commission des finances du Sénat, octobre 2015. Une grande partie de ce coût (propagande, remboursements de campagne) existerait de toute façon, avec ou sans ShadowVote.

Coût de ShadowVote (estimation)

Phase 1 : développement et test pilote (dépense unique)

Poste	Coût
Prototype (développement, audits, juridique)	450 000 €
Test pilote dans une ville volontaire	350 000 à 500 000 €
TOTAL	environ 0,8 à 1 million € (une seule fois)

Phase 2 : fonctionnement annuel

Poste	Coût annuel
Infrastructure (1 000 nœuds, bande passante)	200 000 €
Équipe permanente (5 personnes)	300 000 €
Audits, frais de blockchain,	200 000 €

communication	
TOTAL	environ 700 000 € par an

Comparaison

Système	Coût initial	Coût annuel	Ordre de grandeur
Organisation officielle d'un scrutin national	—	—	≈ 216 M€ par scrutin
ShadowVote (estimation)	≈ 0,8 à 1 M€	≈ 0,7 M€	Moins de 0,5 % du coût d'un seul scrutin national

Soyons précis : le ShadowVote ne remplace pas l'urne, il s'y ajoute. Il ne fait donc économiser aucun argent à l'État. Mais il coûterait chaque année moins d'un demi pour cent du prix d'une seule élection nationale — pour une vérifiabilité que le papier n'offre pas. Le coût n'est pas un obstacle.

CONCLUSION : la technologie existe, il manque la volonté

Vous venez de parcourir les bases de la blockchain. Vous savez désormais :

- Ce qu'est un registre public difficile à falsifier
- Pourquoi la copie multiple protège contre la fraude
- Ce que le pseudonymat protège réellement — et ce qu'il ne garantit pas au sens juridique strict
- Que le coût du ShadowVote resterait marginal comparé à celui d'une élection

La maturité technologique

La technologie n'est pas de la science-fiction :

- Bitcoin fonctionne depuis 2009 : les rares incidents techniques (comme un bug corrigé en quelques heures en 2010) n'ont jamais permis de falsifier son registre.
- Ethereum, l'un des plus grands réseaux blockchain au monde, traite des centaines de millions de transactions chaque année.
- Plusieurs pays s'appuient déjà sur la blockchain dans leurs services publics : l'Estonie, pionnière en la matière, utilise depuis des années une blockchain (la KSI Blockchain) pour garantir l'intégrité de certains registres — santé, justice, entreprises. Précision importante : son vote en ligne (l'i-voting, en place depuis 2005) repose sur un système différent, pas sur cette blockchain. L'Estonie prouve donc

que la blockchain peut fonctionner à l'échelle d'un État — pas encore, à ce jour, qu'elle y a été appliquée au vote lui-même.

C'est un logiciel mature, déployé, éprouvé — même si aucun grand pays n'a encore basé son vote national dessus.

Le vrai obstacle

Le problème n'est pas seulement technique. Il est aussi, largement, politique et organisationnel.

Adopter une technologie qui permettrait à chaque citoyen de vérifier lui-même le déroulement d'un scrutin suppose un changement profond dans la manière dont les institutions rendent compte de leur gestion des élections. Ce n'est pas un obstacle propre à un camp politique : c'est une révolution de méthode, qui demandera du temps, des garde-fous juridiques et une volonté partagée.

Mais rien n'oblige à attendre que cette volonté existe pour commencer à construire, expérimenter, et montrer que c'est possible.

TRANSITION VERS LE CHAPITRE 5

Dans le prochain chapitre, nous allons voir comment fonctionnerait concrètement ShadowVote :

- Les étapes du vote, pas à pas
- L'architecture du système
- Un budget réaliste
- Une feuille de route de développement

Vous allez voir que ce n'est pas un rêve. C'est un projet. Faisable. Dès maintenant.

CHAPITRE 5

LE SHADOWVOTE — ARCHITECTURE DU SYSTÈME

« La différence entre un rêve et un projet, c'est un cahier des charges précis. »

Introduction : du concept à la réalité

Dans le Chapitre 4, vous avez compris ce qu'est la blockchain. Dans ce chapitre, nous allons voir comment ce principe s'appliquerait concrètement au vote — pas dans l'abstrait, mais étape par étape, avec des chiffres et des choix techniques assumés.

Nous allons répondre aux questions les plus concrètes que pose l'idée du ShadowVote :

- Comment voterais-je avec le ShadowVote ?
- Où seraient stockés les votes ?
- Qui contrôlerait le système ?
- Combien cela coûterait-il vraiment ?
- Quelle blockchain utiliser (Ethereum, Polygon, une solution française) ?
- Garde-t-on l'urne papier ?

À la fin de ce chapitre, vous saurez exactement ce qu'il faudrait construire — et à quel prix.

Transparence totale. Soyons honnêtes : le ShadowVote n'existe pas encore. Il n'y a ici ni mensonge, ni promesse en l'air. Ce chapitre est le cahier des charges d'un système à construire, pas la description d'un système qui fonctionne déjà. Chaque montant, chaque échéance, chaque scénario que vous allez lire est une hypothèse de travail, présentée comme telle.

1. Le principe du double-vote de la confiance

L'idée centrale

Le ShadowVote ne remplace pas l'urne papier. **Il la complète.**

Le principe tient en une phrase : vous votez deux fois le même jour, dans deux systèmes indépendants, et on compare ensuite les résultats.

- **Une fois dans l'urne** — c'est le vote officiel, légal, celui qui compte pour la République.
- **Une fois sur la blockchain** — c'est le vote témoin, citoyen, qui ne remplace rien mais qui observe.

Les deux systèmes sont gérés séparément : l'État garde l'entière responsabilité de l'urne, les citoyens gèrent eux-mêmes la blockchain, via des associations, des universités et des volontaires — jamais l'État lui-même. Une fois les deux dépouillements terminés, on les compare :

- **Si les résultats convergent**, la confiance est restaurée : deux systèmes indépendants, gérés par des acteurs différents, avec des technologies différentes, arrivent à la même conclusion. C'est la meilleure preuve de sincérité qu'un scrutin puisse recevoir.
- **Si les résultats divergent**, l'écart déclenche un audit citoyen qui force la transparence — nous verrons plus loin comment.

Pourquoi garder l'urne papier ?

Trois raisons stratégiques justifient ce choix, qui n'a rien d'un compromis timide.

Raison 1 — la transition en douceur. On ne supprime pas l'urne du jour au lendemain : ce serait juridiquement impossible (la Constitution encadre le mode de scrutin), culturellement violent (l'attachement des Français à l'isoloir et au bulletin papier est réel) et politiquement suicidaire pour quiconque le proposerait. Le ShadowVote doit donc s'ajouter progressivement, sans jamais menacer l'existant :

Phase	Utilisateurs ShadowVote	Impact
Phase 1	1 % des électeurs	Test pilote
Phase 2	10 % l'utilisent	Pression morale
Phase 3	50 % l'utilisent	Basculement
Phase 4	L'État l'adopte officiellement	Victoire

On ne détruit pas l'ancien système. On le rend, avec le temps, obsolète.

Raison 2 — la redondance de sécurité. Deux systèmes parallèles, c'est deux fois plus de sécurité, pas deux fois plus de risque. Si la blockchain subit une attaque informatique, l'urne papier reste pleinement valide. Si l'urne papier connaît un problème (erreur de comptage, contestation locale), la blockchain apporte un témoignage indépendant. C'est le principe de l'avion : deux moteurs valent mieux qu'un, non pas parce qu'on doute de chacun d'eux, mais parce qu'aucun système ne devrait reposer sur un seul point de défaillance.

Raison 3 — l'inclusivité. Tout le monde n'a pas de smartphone. Tout le monde ne maîtrise pas le numérique. Garder l'urne papier garantit que personne n'est exclu du vote pour une raison technique. Ceux qui veulent juste voter continuent de voter au bureau, comme toujours. Ceux qui veulent en plus vérifier font le double-vote. Chacun choisit son niveau de vigilance — le ShadowVote est une option, jamais une obligation.

2. Les 5 étapes du vote ShadowVote

Un scénario pour comprendre, pas une prédiction

Avant d'entrer dans le détail, une précision importante s'impose. Ce qui suit est un **scénario pédagogique** : il décrit comment le vote se déroulerait *une fois le système pleinement déployé à l'échelle nationale* — pas ce qui se passera concrètement en 2027. Comme vous le verrez à la section 5, l'échéance réaliste pour 2027 est un pilote limité à quelques dizaines de milliers d'utilisateurs sur des scrutins locaux, pas un déploiement national pour l'élection présidentielle elle-même. Le déploiement à grande échelle, celui que ce scénario imagine, viserait plutôt le cycle électoral suivant.

Pour rendre la mécanique concrète, imaginons donc qu'en 2032, le ShadowVote soit devenu un outil de vote témoin utilisé par plusieurs millions de citoyens lors d'une élection présidentielle. Voici comment se déroulerait ce dimanche d'élection.

Vue d'ensemble de la journée

- **Le matin, chez vous** : vous préparez votre identifiant cryptographique.
- **10h, au bureau de vote** : vous votez dans l'urne (vote officiel) et vous scannez un QR code (enregistrement témoin).
- **10h05, dans l'isoloir ou juste après** : vous confirmez votre choix sur votre téléphone ; le vote sera transmis à la blockchain un peu plus tard dans la journée.
- **Le soir, chez vous (20h)** : vous vérifiez que votre vote est bien enregistré et vous comparez les résultats — urne contre blockchain.
- **Le lendemain** : convergence ou divergence est rendue publique, avec, le cas échéant, une pression morale sur l'État.

Étape 1 : la création de votre identité numérique

Quelques jours ou semaines avant l'élection, vous téléchargez l'application ShadowVote (iOS, Android ou web) et vous créez un compte avec une simple adresse email, utile uniquement pour recevoir des notifications. Le système génère alors automatiquement, pour vous, un identifiant

cryptographique unique — quelque chose comme `SV-FR-2032-8f3e7a2d9c1b5e4f6a8d3c7b2e1f9a4c` : les lettres « SV » pour ShadowVote, « FR » pour la France, « 2032 » pour l'année de l'élection, et une longue suite de caractères qui constitue votre identifiant unique.

En parallèle, l'application génère aussi pour vous une **clé privée** : une information strictement secrète, que vous seul connaissez, et qui ne sera **jamais envoyée à personne, jamais affichée dans l'application après sa création, et jamais stockée sur les serveurs de ShadowVote**. C'est elle qui vous permettra, au moment de voter, de prouver que l'identifiant vous appartient — sans jamais révéler qui vous êtes, et sans que la clé elle-même circule où que ce soit. Nous expliquons précisément comment cela fonctionne dans l'encadré technique qui suit.

L'application ne demande jamais votre nom, votre prénom, votre adresse ou votre carte d'identité. Elle demande seulement un email, pour vous notifier que votre vote a bien été enregistré. Avec un email personnel classique, votre fournisseur de messagerie — pas ShadowVote — pourrait en théorie faire un lien entre cette adresse et votre identité. Si vous souhaitez un anonymat renforcé, rien ne vous empêche d'utiliser un email jetable (type TempMail ou Guerrilla Mail) : dans ce cas, personne, pas même votre fournisseur de messagerie, ne pourra relier votre identifiant cryptographique à votre identité réelle.

Pour aller plus loin (technique) — comment une signature prouve une identité sans révéler la clé privée

C'est le point le plus important à bien comprendre, car une confusion ici serait une faille grave : **la clé privée ne quitte jamais votre téléphone**. Elle ne transite jamais sur le réseau, elle n'apparaît jamais dans une base de données, elle n'est jamais visible dans le registre public.

Ce qui circule, en revanche, c'est une **signature cryptographique** — une empreinte numérique *calculée à partir de* votre clé privée et du contenu exact de votre vote, grâce à un algorithme de signature standard (par exemple ECDSA, le même type d'algorithme utilisé pour sécuriser Bitcoin ou les cartes bancaires à puce). Cette signature a trois propriétés essentielles :

- elle est différente à chaque vote, même effectué avec la même clé, car elle dépend aussi du contenu signé ;
- n'importe qui peut vérifier, avec votre identifiant public, que la signature est authentique ;
- **personne ne peut, à partir de la signature, retrouver la clé privée qui l'a produite** — la relation ne fonctionne que dans un sens.

C'est exactement le même principe qu'une signature manuscrite au bas d'un chèque : la signature prouve que c'est vous qui avez signé, sans que quiconque ait besoin de connaître le mouvement exact de votre main pour la vérifier.

Dans un exemple concret, votre clé privée secrète pourrait ressembler à ``7d3f8a2c9e1b4f6a8d2c7e3b9f1a5c4e`` — un secret que vous seul détenez et qui ne sort jamais de votre appareil. La signature qui en est *dérivée* pour un vote donné ressemblerait, elle, à ``b2f4c8a1d6e3f9b7a5c2e8d4f1b6a9c3`` : une valeur totalement différente, propre à ce vote précis, et c'est **cette seule valeur** qui apparaît dans le paquet envoyé à la blockchain et dans le registre public.

Étape 2 : vous vous rendez au bureau de vote

Dimanche, 10h, élection présidentielle. Vous allez au bureau de vote et vous faites exactement comme d'habitude : vous présentez votre carte d'électeur, vous signez la liste d'émargement, on vous donne des bulletins et une enveloppe, vous passez dans l'isoloir. Jusqu'ici, absolument rien ne change.

Étape 3 : dans l'isoloir, le double-vote

Vous êtes dans l'isoloir, vos bulletins devant vous. Le geste classique reste inchangé : vous choisissez votre candidat et vous glissez le bulletin dans l'enveloppe, qui ira dans l'urne — c'est le vote officiel.

À côté, un second geste, propre au ShadowVote, vient s'ajouter. Deux façons de procéder sont envisagées :

- **Option A — bureau de vote équipé (solution idéale)** : le bureau affiche, sur un écran ou une affiche plastifiée, un QR code propre à ce bureau, contenant le code du bureau, la liste des candidats et l'heure. Vous le scannez avec l'application.
- **Option B — vous le faites vous-même (solution de transition)** : vous ouvrez l'application sur votre téléphone, vous sélectionnez votre candidat et vous confirmez.

Dans les deux cas, l'application note alors trois choses sur votre téléphone, et rien d'autre : **qui vote** (votre identifiant), **pour qui** (votre choix) et **à quelle heure** (l'horodatage). Le détail technique exact de cet enregistrement figure dans l'encadré ci-dessous, pour les lecteurs curieux.

Ce vote n'est cependant **pas encore envoyé** à la blockchain à ce stade — pour une raison de bon sens : si des dizaines de millions d'électeurs envoyaient leur vote au même instant entre 8h et 20h, cela créerait un

embouteillage réseau. Le vote reste donc stocké temporairement, chiffré, sur votre téléphone.

Étape 4 : vous sortez de l'isoloir et vous votez dans l'urne

Vous sortez, vous glissez votre enveloppe dans l'urne — c'est le vote officiel — et le président du bureau prononce le traditionnel « A voté ! ». Vous rentrez chez vous.

C'est en sortant du bureau, ou plus tard dans la journée, dès que vous disposez d'une connexion internet stable, que l'application envoie automatiquement votre vote à la blockchain. Votre téléphone se connecte alors à plusieurs nœuds du réseau ShadowVote et transmet un paquet chiffré contenant votre identifiant, votre choix, l'horodatage et la signature cryptographique décrite plus haut — **jamais votre clé privée elle-même**.

Les nœuds du réseau vérifient alors trois choses : que cet identifiant n'a pas déjà voté, que la signature est valide, et que le candidat choisi existe bien. Si tout est en ordre, le vote est ajouté au bloc en cours de constitution ; une fois ce bloc rempli (dix mille votes, par exemple), il est scellé et ajouté définitivement à la chaîne.

Vous recevez alors une notification — votre **reçu de vote** — de ce type : « *Votre vote a été enregistré dans la blockchain ShadowVote. Identifiant : SV-FR-2032-8f3e7a... | Bloc n° 47832.* » Ce reçu fonctionne comme un ticket de carte bancaire : vous pouvez le garder et le vérifier, mais vous ne pouvez pas vous en servir pour prouver à quelqu'un d'autre pour qui vous avez voté — c'est une protection essentielle contre l'achat de vote.

Pour aller plus loin (technique) — ce que contiennent vraiment les fichiers

L'enregistrement local, sur votre téléphone, avant tout envoi, se présente ainsi :

```
{  
  "identifiant": "SV-FR-2032-8f3e7a...",  
  "choix": "CandidatX",  
  "horodatage": "2032-04-11 10:23:47"  
}
```

Le paquet effectivement transmis aux nœuds de la blockchain, lui, ajoute la signature dérivée de votre clé privée — jamais la clé elle-même :

```
{  
  "identifiant": "SV-FR-2032-8f3e7a2d...",
```

```

"vote": "CandidatX",
"timestamp": "2032-04-11 10:23:47",
"signature": "b2f4c8a1d6e3f9b7a5c2e8d4f1b6a9c3"
}

```

Notez la différence essentielle avec la clé privée de l'exemple précédent (`7d3f8a2c9e1b4f6a8d2c7e3b9f1a5c4e`) : ce sont deux valeurs distinctes, et seule la seconde — la signature — voyage sur le réseau et devient publique.

Étape 5 : vous vérifiez, le soir de l'élection

20h. Les bureaux ferment, le dépouillement commence. Pendant que les assesseurs comptent les bulletins papier — le résultat officiel —, vous ouvrez l'application ShadowVote, qui vous propose trois choses.

Vérifier votre propre vote. Vous entrez votre identifiant, ou vous scannez votre reçu ; l'application interroge la blockchain et vous confirme que votre vote a bien été trouvé dans le bloc annoncé, à l'heure attendue, pour le candidat que vous avez choisi. Vous disposez ainsi de la preuve que votre vote a été compté.

Consulter les résultats ShadowVote en temps réel. Un exemple, purement fictif, de ce que l'application pourrait afficher à 20h37 :

Candidat	Pourcentage	Votes
Candidat X	51,2 %	3 676 160
Candidat Y	27,5 %	1 974 500
Candidat Z	12,9 %	926 220
Autres	8,4 %	603 120

Total des votes ShadowVote enregistrés : 7 180 000, sur un corps électoral de plusieurs dizaines de millions d'inscrits.

À 20h45, le ministère de l'Intérieur annonce les résultats officiels de l'urne — toujours dans notre exemple fictif : Candidat X 51,4 %, Candidat Y 27,3 %, Candidat Z 12,8 %.

Comparer les deux résultats. L'application produit alors automatiquement un tableau comparatif :

Candidat	Urne officielle	ShadowVote	Écart
X	51,4 %	51,2 %	−0,2
Y	27,3 %	27,5 %	+0,2
Z	12,8 %	12,9 %	+0,1

Écart moyen : environ 0,15 point. Verdict : **convergence**. Les deux systèmes, indépendants, arrivent à un résultat quasi identique. La confiance est restaurée.

Scénario alternatif : la divergence

Imaginons maintenant, toujours à titre d'exemple fictif, que les résultats divergent nettement :

Candidat	Urne officielle	ShadowVote	Écart
X	51,4 %	44,9 %	−6,5
Y	27,3 %	33,8 %	+6,5
Z	12,8 %	12,6 %	−0,2

Écart moyen : environ 3,3 points. Verdict : **divergence significative**. Que se passerait-il alors ?

Phase 1 — alerte citoyenne. L'application déclenche une alerte du type : « *Écart de 3,3 points détecté entre l'urne et la blockchain. Ceci nécessite un audit.* » Des milliers de citoyens la reçoivent au même moment.

Phase 2 — pression médiatique. Les réseaux sociaux s'emparent du sujet, les médias relaient l'information, le ministère de l'Intérieur est mis en demeure de réagir.

Phase 3 — trois options pour l'État.

- *Recompter l'urne.* Un recomptage manuel est ordonné. S'il confirme l'urne, l'écart provient probablement d'un biais du côté du ShadowVote — nous y revenons ci-dessous. S'il confirme le ShadowVote, une erreur, voire une fraude, est mise au jour dans le système officiel.
- *Ignorer.* L'État peut refuser de recompter en affirmant que le ShadowVote n'a aucune valeur légale. Le problème est alors politique : des millions de citoyens détiennent une preuve cryptographique qu'une divergence existe, et la légitimité du scrutin s'en trouve entachée.
- *Adopter officiellement le ShadowVote.* L'État reconnaît la valeur du dispositif et propose de l'intégrer au processus officiel pour les élections suivantes.

Il faut être honnête sur un point que le triptyque ci-dessus ne doit pas masquer : **une divergence ne prouve pas automatiquement une fraude dans l'urne**. Les utilisateurs du ShadowVote, à ce stade de son développement, seraient probablement plus jeunes, plus connectés et plus politisés que la moyenne de l'électorat — un biais d'échantillon qui peut, à lui seul, expliquer une partie de l'écart, sans qu'aucune manipulation n'ait eu lieu nulle part. C'est précisément pour cette raison que la divergence doit déclencher un audit, et non une accusation immédiate : le rôle du ShadowVote est de poser la question, pas d'y répondre à la place des institutions compétentes.

Dans tous les cas, le dispositif remplit sa fonction : soit il confirme que le système officiel fonctionne, soit il révèle une question qui méritait d'être posée. La transparence l'emporte toujours.

3. Architecture technique du système

Le système ShadowVote reposerait sur quatre briques techniques, empilées les unes sur les autres :

1. **L'application mobile et web** — l'interface que voit l'utilisateur. 2. **Le réseau de nœuds** — le cœur décentralisé de la blockchain. 3. **Le registre public** — la base de données où sont conservés les votes. 4. **Les outils d'audit** — les instruments qui permettent aux citoyens d'exercer un contrôle réel.

Composante 1 : l'application

Côté technique, on envisagerait un développement mobile en React Native (une seule base de code pour iOS et Android) et un site web en React.js, accessible depuis n'importe quel navigateur, avec un niveau d'ergonomie comparable à celui d'une application bancaire. Ses fonctionnalités couvriraient la création d'identité cryptographique, le scan de QR code (ou la sélection manuelle), l'envoi chiffré du vote, la vérification personnelle et la consultation des résultats et de leur comparaison avec l'urne. L'interface serait proposée au minimum en français et en anglais, avec d'autres langues selon les pays qui souhaiteraient adopter le système.

Composante 2 : le réseau de nœuds

Un nœud est simplement un serveur qui participe à la blockchain : il reçoit les votes, vérifie leur signature et leur unicité, les ajoute au registre et conserve une copie complète de la chaîne. L'objectif viserait plus d'un millier de nœuds décentralisés, gérés non pas par l'État mais par un ensemble d'acteurs indépendants : associations citoyennes, universités menant des recherches en cryptographie, ONG de transparence, collectivités locales volontaires et citoyens eux-mêmes, sur le modèle déjà éprouvé par Bitcoin. Aucun nœud n'appartiendrait à l'État central — c'est une condition de crédibilité du dispositif, pas un détail technique.

Trois options technologiques ont été comparées.

	Avantages	Inconvénients
Ethereum (blockchain publique existante)	Blockchain la plus mature ; large communauté de développeurs ;	Coût par transaction élevé (de l'ordre de 0,50 € à 5 €) ; débit limité (environ 15

	infrastructure déjà en place ; open-source	transactions/seconde) — trop cher et trop lent pour un scrutin national
Polygon (réseau secondaire compatible Ethereum)	Compatible avec l'écosystème Ethereum ; coût très inférieur (de l'ordre de 0,001 €/transaction) ; débit bien plus élevé (plusieurs centaines de transactions par seconde en pratique) ; déjà utilisé par de grandes plateformes grand public	Moins décentralisé qu'Ethereum ; dépend, in fine, de la gouvernance d'Ethereum et de la fondation Polygon
Blockchain sur mesure (développée spécifiquement)	Contrôle total ; optimisée pour le vote ; aucun coût de transaction récurrent ; peut être entièrement française ou européenne	Développement long (de l'ordre de 12 à 18 mois) ; coût initial élevé ; moins d'auditeurs externes indépendants au démarrage

Ethereum, en l'état, n'est pas adapté à un scrutin national : trop cher, trop lent à l'échelle de plusieurs millions de votes. Une blockchain sur mesure serait l'option la plus satisfaisante à long terme, mais son développement est trop lent pour démarrer rapidement. Polygon apparaît donc comme l'option recommandée pour un déploiement initial rapide, avec un coût estimé — à titre d'ordre de grandeur, pour un scrutin mobilisant plusieurs dizaines de millions de votes — de quelques dizaines de milliers d'euros, contre plusieurs dizaines de millions d'euros sur Ethereum. Ce choix n'est toutefois pas sans risque à surveiller : dépendre de Polygon, c'est dépendre aussi de sa gouvernance, d'une éventuelle évolution de sa politique de frais, et du cadre réglementaire européen sur les crypto-actifs (le règlement MiCA), qui pourrait, à terme, imposer des contraintes nouvelles à ce type d'infrastructure.

Notre recommandation stratégique tient donc en deux phases : une **Phase 1 (2026-2027)** sur Polygon, pour un déploiement rapide à coûts faibles à des fins de test et de pilote — et non de déploiement présidentiel national, comme précisé à la section 5 — puis une **Phase 2 (à partir de 2028)**, une fois le mouvement établi, consacrée au développement progressif d'une blockchain souveraine, française ou européenne.

Composante 3 : le registre public

C'est l'endroit où tous les votes seraient conservés de manière définitive et infalsifiable. En langage courant, chaque vote enregistré dans le registre porterait : le numéro du bloc auquel il appartient, l'heure exacte de son enregistrement, l'identifiant anonyme de l'électeur, le candidat choisi, une empreinte de sécurité — la signature décrite plus haut — et un lien cryptographique vers le vote précédent, qui garantit qu'aucune modification n'est possible après coup sans que cela se voie immédiatement.

Pour aller plus loin (technique) — la structure d'un vote dans le registre

```
{
  "bloc": 47832,
  "timestamp": "2032-04-11T10:24:03Z",
  "identifiant": "SV-FR-2032-8f3e7a2d9c1b5e4f6a8d3c7b2e1f9a4c",
  "vote": "CandidatX",
  "signature": "b2f4c8a1d6e3f9b7a5c2e8d4f1b6a9c3",
  "hash_precedent": "3a5f7c9d2e1b8f4a6c3e9d7b2f1a5c8e"
}
```

Comme dans le paquet envoyé au moment du vote, le champ `signature` contient une empreinte *dérivée* de la clé privée de l'électeur — jamais la clé elle-même. **La clé privée ne figure et n'a jamais figuré à aucun endroit du registre.** C'est cette distinction qui rend le registre public sans compromettre le secret de chaque électeur.

Ce que le registre rend visible à tous, et ce qu'il ne révèle à personne, peut se résumer ainsi :

Ce que tout le monde peut voir	Ce que personne ne peut voir
Qu'un vote a été enregistré	Qui est cette personne dans la vraie vie
L'identifiant anonyme qui a voté	Son nom, son prénom, son adresse
Le candidat choisi	—
L'horodatage du vote	—

En termes de volume, chaque vote occuperait environ 200 octets ; à l'échelle de plusieurs dizaines de millions de votes, le registre complet resterait de l'ordre de quelques gigaoctets seulement — sans commune mesure avec la blockchain Bitcoin (plusieurs centaines de gigaoctets) ou, a fortiori, avec les infrastructures de stockage d'un service comme Netflix. Le registre ShadowVote tiendrait, dans son intégralité, sur une simple clé USB.

Composante 4 : les outils d'audit, le pouvoir citoyen

Quatre outils permettraient aux citoyens d'exercer un contrôle réel et non symbolique sur le système :

- **Le vérificateur individuel**, qui permet à chacun de retrouver son propre vote à partir de son identifiant.
- **L'explorateur de blockchain**, sorte de moteur de recherche du registre, qui permet de consulter tous les blocs, tous les votes (sous forme d'identifiants anonymes), de vérifier l'intégrité des empreintes cryptographiques et de télécharger la base de données complète.
- **Le comparateur urne/blockchain**, un tableau de bord public affichant en temps réel les résultats ShadowVote, les résultats officiels une fois annoncés, les écarts par candidat et, le cas échéant, une cartographie des divergences par région.
- **Le détecteur d'anomalies**, un algorithme chargé de repérer les pics de votes suspects, les tentatives de vote en double sur un même identifiant, et les votes déposés hors délai.

4. Budget réaliste et transparent

Avertissement méthodologique. Les montants qui suivent sont des **estimations de travail**, pas un budget arrêté ni un devis contractuel. Ils ont été construits par comparaison avec des projets civic-tech de taille et de complexité comparables (applications citoyennes à grande échelle, plateformes de vote vérifiable, outils de transparence démocratique), en appliquant des ratios usuels du secteur du développement logiciel et de la sécurité informatique. Ils ont pour seule vocation de donner un **ordre de grandeur crédible**, permettant de juger si le projet est réaliste financièrement — pas de servir de base à un engagement financier précis. Seuls des devis réels, obtenus auprès de prestataires identifiés, pourraient affiner ces chiffres.

Phase 1 : développement du prototype (6 à 12 mois, estimation)

Poste	Détail	Coût estimé
Développement logiciel	2 développeurs full-stack × 6 mois	180 000 €
Développement blockchain	1 développeur blockchain × 6 mois	90 000 €
Design UX/UI	1 designer × 3 mois	30 000 €
Audit de sécurité	Cabinet externe (2 audits)	80 000 €

Infrastructure cloud	Serveurs de test	20 000 €
Juridique	Consultations d'avocat	30 000 €
Communication	Site web, documentation	20 000 €
Total Phase 1 (estimation)		450 000 €

Phase 2 : test pilote (6 à 12 mois, estimation)

Poste	Détail	Coût estimé
Recrutement de testeurs	10 000 utilisateurs pilotes	50 000 €
Infrastructure de production	100 nœuds décentralisés	100 000 €
Support utilisateurs	Hotline, FAQ, tutoriels	50 000 €
Maintenance logicielle	Corrections de bugs, mises à jour	50 000 €
Campagne de communication	Médias, réseaux sociaux	100 000 €
Total Phase 2 (estimation)		350 000 €

Phase 3 : déploiement à plus grande échelle (12 mois et plus, coût annuel estimé)

Poste	Détail	Coût annuel estimé
Infrastructure	1 000 nœuds et bande passante	200 000 €
Équipe permanente	5 personnes (développement et support)	300 000 €
Frais de blockchain	Transactions Polygon	50 000 €
Audits annuels	Sécurité et conformité légale	50 000 €
Communication	Campagnes, partenariats	100 000 €
Total annuel (estimation)		700 000 €/an

Budget total sur 3 ans (estimation)

Phase	Coût estimé
Développement du prototype	450 000 €

Test pilote	350 000 à 500 000 € (voir chapitre 9)
Année 1 de déploiement	700 000 €
Année 2	700 000 €
Année 3	700 000 €
Total 3 ans (estimation)	environ 2,9 à 3,1 millions €

À titre de comparaison d'ordre de grandeur, le coût habituellement avancé pour l'organisation d'**une seule** élection présidentielle française se compte en centaines de millions d'euros. Même en tenant compte de la marge d'incertitude propre à ce type d'estimation, l'écart d'échelle entre les deux budgets reste considérable — c'est cet ordre de grandeur, plus que le chiffre au euro près, qui constitue l'argument à retenir.

Financement : comment le payer ?

Phase 1 — crowdfunding citoyen. Un objectif de l'ordre de 450 000 € pourrait, en théorie, être atteint par 45 000 citoyens contribuant 10 € chacun, ou 4 500 contribuant 100 €, ou toute combinaison intermédiaire, sur le modèle d'une plateforme comme Kickstarter ou Ulule, avec remboursement automatique si l'objectif n'est pas atteint.

Phase 2 — subventions et mécénat. Plusieurs pistes de financement sont envisageables à ce stade, **à titre purement illustratif du type d'acteurs qui financent habituellement ce genre de projets civic-tech** : des fondations engagées dans le soutien à la démocratie (par exemple des structures comparables à Open Society Foundations ou à la Fondation Ford), des fonds européens dédiés à l'innovation démocratique, ou des philanthropes du secteur technologique déjà connus pour financer des projets de transparence civique (Pierre Omidyar, fondateur d'eBay, en est un exemple public). **Il s'agit de pistes de financement envisageables, non encore approchées ni engagées à ce jour** : aucune de ces personnes ou organisations n'a été contactée au sujet du ShadowVote, et leur mention ici ne suppose ni intérêt, ni soutien, ni lien d'aucune sorte avec le projet.

Phase 3 — modèle associatif ou fondation. La structure légale porteuse du projet pourrait prendre la forme d'une association loi 1901, d'une fondation reconnue d'utilité publique, ou d'une coopérative citoyenne, avec un conseil d'administration élu par les contributeurs, une transparence financière totale (comptes publics) et l'absence de tout objectif de profit — le budget ne couvrant que les coûts réels de fonctionnement.

5. Feuille de route technique

Transparence absolue. Nous ne prétendons pas que le ShadowVote existe. Voici, trimestre par trimestre, ce qu'il faudrait faire pour le construire — et une précision essentielle avant de commencer : l'échéance de 2027 mentionnée dans cette feuille de route correspond à un objectif de **prototype et de pilote limité**, ainsi qu'à un jalon de pression politique — pas à un déploiement national pour l'élection présidentielle elle-même. Le déploiement à grande échelle, celui qui concernerait plusieurs millions d'électeurs, viserait le cycle électoral suivant.

Trimestres 1-2 (mois 1 à 6) : développement

- **Livrable 1 — application mobile (iOS/Android)** : inscription, création d'identité cryptographique, interface de vote, vérification.
- **Livrable 2 — smart contracts (sur Polygon)** : contrat de vote, contrat de validation, contrat d'audit.
- **Livrable 3 — backend et API** : serveur assurant la communication entre l'application et la blockchain, système de notifications, base de données des utilisateurs limitée aux emails (aucune identité réelle).
- **Livrable 4 — explorateur de blockchain** : site public permettant de consulter tous les votes, avec un outil de recherche par identifiant et un téléchargement de la base complète.

Trimestre 3 (mois 7 à 9) : tests et audits

- **Audit de sécurité n°1** : confié à un cabinet externe spécialisé dans l'audit de systèmes blockchain — des structures du type de celles qui interviennent habituellement dans ce secteur, à titre d'exemple du profil recherché, sans qu'aucun mandat ne soit à ce jour engagé — comprenant tests d'intrusion, audit du code source et corrections des failles détectées.
- **Tests utilisateurs** : environ 1 000 bêta-testeurs, vote test sur un sujet fictif, recueil de retours d'expérience.
- **Audit juridique** : conformité au RGPD, statut légal du vote parallèle, protection des données personnelles.

Trimestre 4 (mois 10 à 12) : le pilote

L'objectif de cette phase serait de réunir environ 10 000 utilisateurs autour d'un vote test portant sur un sujet réel mais non électoral au sens strict — un référendum local de budget participatif, par exemple. La ville pilote idéale présenterait une population jeune et connectée, un exécutif municipal ouvert à l'innovation, et une taille moyenne (de l'ordre de 50 000 à 150 000 habitants), avec un budget participatif déjà en place. Aucune ville n'a été contactée à ce stade.

Le déroulement serait le suivant : les citoyens votent normalement, dans l'urne ou via le dispositif local existant ; ceux qui le souhaitent utilisent en parallèle le ShadowVote ; les deux résultats sont comparés. On mesurerait ainsi le taux d'adoption, la facilité d'usage, la fiabilité technique du système et l'ampleur des écarts éventuels — c'est précisément ce pilote, et non un déploiement présidentiel, qui correspond à l'échéance réaliste de 2027.

Année 2 : déploiement progressif

Une fois les enseignements du pilote intégrés (corrections techniques au premier trimestre, lancement médiatique national au deuxième), le système pourrait être proposé, en parallèle du vote officiel, lors d'élections régionales ou départementales, avec un objectif de l'ordre de 100 000 utilisateurs, soit une fraction encore modeste du corps électoral.

Année 3 et au-delà : vers le basculement

L'objectif de long terme, mesuré non plus en dizaines de milliers mais en millions d'utilisateurs, viserait le cycle électoral suivant — l'échéance présidentielle qui succède à celle de 2027. C'est à cette échelle, et seulement à cette échelle, que le triptyque convergence/divergence décrit à la section 2 prendrait tout son sens politique : pression morale sur l'État, couverture médiatique massive, débat politique national et, en bout de course, une éventuelle proposition de loi d'intégration officielle du dispositif.

Conclusion : ce n'est pas un rêve, c'est un cahier des charges

Ce chapitre vous a montré comment le ShadowVote fonctionnerait (le double-vote en cinq étapes), sur quoi il reposerait techniquement (une blockchain Polygon dans un premier temps, une infrastructure souveraine ensuite), combien cela coûterait selon une estimation raisonnable (de l'ordre de 450 000 € pour le développement, puis 700 000 € par an en exploitation), qui pourrait le financer (crowdfunding, fondations, subventions — sans qu'aucun de ces financements ne soit à ce jour engagé) et selon quel calendrier réaliste il pourrait voir le jour : un pilote limité à l'horizon 2027, un déploiement à grande échelle visant le cycle électoral suivant.

Le ShadowVote n'existe pas encore. Mais rien, dans ce chapitre, n'indique qu'il relève de la science-fiction : chaque brique décrite ici s'appuie sur des technologies qui existent déjà et fonctionnent à grande échelle ailleurs. Ce qui manque n'est pas la technique. C'est la décision de s'y mettre.

Dans le prochain chapitre, nous répondrons aux dernières objections techniques : la sécurité face aux tentatives d'attaque, les garanties

d'anonymat, l'accessibilité pour tous les publics, et un comparatif de coûts plus détaillé encore. Vous verrez qu'il ne reste, à ce stade, plus guère d'obstacle technique — seulement une question de volonté politique.

CHAPITRE 6

SÉCURITÉ, ANONYMAT, ACCESSIBILITÉ

« Un système démocratique sans sécurité, sans anonymat et sans accessibilité n'est pas démocratique. »

Introduction : les quatre piliers non négociables

Le ShadowVote peut avoir la meilleure architecture technique du monde (Chapitre 5) — si les questions suivantes ne trouvent pas de réponse solide, le système échoue, quel que soit par ailleurs le soin apporté à sa conception :

- **Sécurité** : peut-on pirater le système ?
- **Anonymat** : mon vote restera-t-il protégé ?
- **Accessibilité** : ma grand-mère de 87 ans pourra-t-elle l'utiliser ?
- **Coût** : est-ce que ça vaut vraiment le coup, financièrement ?

Ce sont les quatre piliers sur lesquels reposera, ou s'effondrera, la crédibilité du ShadowVote. Les trois premiers sont des conditions de légitimité : un système qu'on ne peut pas sécuriser, dont on ne peut pas protéger le contenu, ou que seule une minorité de citoyens équipés et formés peut utiliser, ne mérite pas le nom de vote démocratique. Le quatrième est une condition de faisabilité politique : même une solution techniquement irréprochable ne convaincra personne si son coût paraît disproportionné au regard de ce qu'elle apporte.

Ce chapitre répond aux quatre avec des faits, des chiffres sourcés quand ils existent, des estimations clairement identifiées comme telles quand aucune source fiable n'est disponible, et des comparaisons systématiques avec l'urne papier. Nous ne chercherons pas à masquer les limites réelles du système : un chapitre qui prétendrait à la perfection totale serait plus fragile, pas plus solide, face au premier lecteur averti. À la fin de ce chapitre, vous saurez que le ShadowVote est :

- **Plus sûr** que l'urne papier sur la plupart des critères, avec des limites assumées ;
- **Solidement pseudonymisé** — comparable au bulletin traditionnel sur l'essentiel, avec une nuance technique importante que nous allons expliquer sans détour ;
- **Plus accessible** qu'on ne le pense, à condition d'investir dans la formation et l'accompagnement ;
- **D'un coût marginal** comparé à celui d'une élection, sans prétendre faire économiser de l'argent tant que l'urne reste en place.

1. Sécurité : plus robuste que vous ne le craignez

La question qui tue

« D'accord, c'est bien joli votre blockchain. Mais si des hackers russes, chinois ou nord-coréens décident de pirater le système, qu'est-ce qui les en empêche ? »

Réponse courte : l'architecture du réseau, la cryptographie, et — nous allons y venir — la gouvernance humaine qui l'entoure.

Réponse longue : lisez ce qui suit.

Ce que l'histoire nous apprend (et pourquoi il faut en tenir compte)

Avant de détailler les parades du ShadowVote, une honnêteté s'impose : le vote électronique et le vote par blockchain ont déjà connu des échecs retentissants ailleurs, et les ignorer serait la meilleure façon de perdre toute crédibilité auprès d'un lecteur informé.

En 2019, la Poste suisse a suspendu le déploiement à grande échelle de son système de vote électronique après qu'une équipe internationale de chercheurs, invitée à l'auditer publiquement avant sa généralisation, a découvert des failles cryptographiques critiques permettant en théorie de falsifier des votes sans laisser de trace détectable. La même année, le chercheur français Pierrick Gaudry a démontré qu'il pouvait retrouver le contenu de votes soi-disant chiffrés dans le système de vote par blockchain testé par la ville de Moscou pour des élections locales — en une vingtaine de minutes. Ces deux épisodes ne sont pas des anecdotes isolées : ils illustrent une réalité têtue, régulièrement rappelée par des cryptographes académiques comme J. Alex Halderman (université du Michigan) ou Ronald Rivest (MIT, l'un des inventeurs de RSA) — construire un système de vote à distance qui soit à la fois sûr, secret et vérifiable figure parmi les problèmes non résolus les plus difficiles de la cryptographie appliquée, et aucune solution ne fait aujourd'hui consensus pour remplacer purement et simplement un scrutin officiel et contraignant.

C'est précisément pour cette raison que le ShadowVote ne se présente pas comme un remplacement du système d'État. La Suisse et Moscou avaient l'une et l'autre engagé l'autorité officielle sur un scrutin contraignant : la moindre faille y avait des conséquences juridiques et politiques immédiates. Le ShadowVote, lui, se positionne dès le départ comme un **vote parallèle citoyen, non officiel** (voir Chapitres 5 et 9) : son rôle, dans un premier temps, est de produire une preuve de participation vérifiable et un signal politique — pas de se substituer du jour au lendemain au bulletin dans l'urne. Cette prudence n'est pas un aveu de faiblesse, c'est une condition de sérieux : elle permet de faire auditer le code en continu par la communauté

(programme de bug bounty, audits indépendants publiés), de corriger les failles avant qu'elles ne soient exploitées à grande échelle, et de n'envisager une intégration officielle qu'au rythme du pilote local décrit aux chapitres 5 et 9 — pas dans la précipitation qui a coûté cher à d'autres.

Les cinq types d'attaques possibles (et leurs parades)

ATTAQUE #1 : Le piratage de la blockchain elle-même

Objectif de l'attaquant : modifier des votes déjà enregistrés dans la blockchain — par exemple, changer un million de votes du Candidat X en votes pour le Candidat Y.

Précision d'architecture indispensable. Le ShadowVote (Chapitre 5) utilise une technologie compatible Polygon — une blockchain fonctionnant en **Proof-of-Stake** (preuve d'enjeu), et non en Proof-of-Work (preuve de travail, le mécanisme de Bitcoin fondé sur une course de calcul). Cette distinction change tout dans la façon de penser une attaque, et il faut aussi être clair sur un second point : le ShadowVote ne se contente pas de brancher ses votes sur le réseau public Polygon partagé par des milliers d'applications. Il s'appuie sur un **réseau de validateurs dédié**, techniquement compatible avec l'écosystème Polygon/Ethereum, mais dont les nœuds sont des entités identifiées et auditées — universités, associations de lutte contre la corruption, organismes d'observation électorale internationaux, ordres professionnels d'audit, partis politiques volontaires — sélectionnées et renouvelées selon la gouvernance multipartite décrite au Chapitre 7 (le réseau des Sentinelles et de leurs partenaires institutionnels). Ce choix a un coût : avec une centaine de validateurs identifiés au lancement (objectif 1000+ à terme), le réseau du ShadowVote est plus petit, donc en théorie plus facile à capturer financièrement, que le réseau public Polygon qui compte des centaines de validateurs adossés à des milliards de dollars d'enjeux. C'est le prix d'un système dont on connaît et peut auditer chaque opérateur — un compromis assumé, pas un point aveugle.

Comment fonctionnerait une capture à 51 % en Proof-of-Stake. Sur une chaîne PoS, un attaquant qui prend le contrôle de la majorité des validateurs (51 % des voix de validation, ou une minorité de blocage selon les paramètres retenus) ne « gagne pas une course de calcul » comme sur Bitcoin : il devient, à partir de ce moment, en mesure de proposer et de valider des blocs frauduleux. La vraie question n'est donc pas « peut-il aller plus vite que le réseau honnête ? » — il n'y a pas de course — mais « que se passe-t-il une fois qu'il a pris la majorité ? ». Et c'est là que le modèle de menace change radicalement par rapport au Bitcoin de nos grands-parents numériques.

Estimation du coût d'une capture (réseau dédié ShadowVote, ~100 validateurs au lancement) :

Composant	Prix unitaire estimé	Quantité nécessaire	Total estimé
Corruption ou rachat d'une entité validatrice identifiée	~10 000 € (<i>estimation</i>)	51 entités	~510 000 €
Constitution des positions de mise en jeu (staking)	Variable	51 positions	~500 000 €+ (<i>estimation</i>)
Total estimé			de l'ordre de 1 million €

Ce chiffre paraît, à première vue, largement à portée d'un État hostile — et il faut le dire clairement plutôt que le minimiser. Mais un budget suffisant ne suffit pas à réussir l'attaque, pour trois raisons qui n'ont rien à voir avec une « course de calcul » :

1. Le slashing — la sanction économique automatique. Le protocole Proof-of-Stake intègre un mécanisme de *slashing* : tout validateur qui signe des blocs contradictoires, invalide, ou en dehors des règles du consensus voit sa mise (le capital qu'il a immobilisé pour devenir validateur) automatiquement confisquée par le protocole, sans intervention humaine. Autrement dit, l'attaque est en partie auto-punitive : au moment précis où la fraude devient détectable — et elle le devient dès qu'un seul autre validateur ou un nœud d'observation constate la divergence —, l'attaquant perd une partie substantielle de ce qu'il vient d'investir. Ce n'est plus « voler discrètement », c'est « payer très cher pour un vol qui explose entre les mains de celui qui le commet ».

2. La réplication massive rend la falsification visible, pas invisible. Reprenons l'image du livre scellé, en la corrigeant : chaque bloc est bien scellé par un sceau qui dépend du bloc précédent. Mais la défense n'est plus « personne ne peut recalculer les sceaux plus vite que le réseau honnête » — ce serait vrai pour Bitcoin, pas pour le ShadowVote. La vraie défense est que des **milliers de copies indépendantes** de ce livre existent déjà : chez des citoyens, des journalistes, des partis d'opposition, des observateurs internationaux, des chercheurs universitaires — tous peuvent faire tourner un nœud complet et vérifier eux-mêmes l'historique (Chapitre 5, Composante 4). Réécrire une page du passé ne suffit pas : il faudrait convaincre — ou faire taire — chacune de ces copies indépendantes, ce qui est une opération de falsification à grande échelle, publiquement vérifiable, et non un problème de puissance de calcul.

3. La réponse sociale et politique — le dernier rempart, assumé comme tel. Si, malgré le slashing et la réplication, une majorité hostile

parvenait à imposer une version frauduleuse de la chaîne, la réponse ultime ne serait pas mathématique mais humaine et institutionnelle : un *hard fork* — une bifurcation du réseau décidée collectivement par les Sentinelles, les institutions partenaires et la communauté des observateurs (Chapitre 7) — qui rejette la branche frauduleuse et fait repartir la chaîne légitime à partir du dernier bloc sain. C'est exactement ce qui s'est produit dans l'écosystème Ethereum en 2016 après le piratage du « DAO » : la communauté a collectivement choisi de créer une nouvelle branche annulant les effets du piratage. Ce n'est pas une garantie automatique et instantanée — c'est une garantie de dernier recours, qui suppose une gouvernance vigilante et légitime. C'est précisément la raison pour laquelle le Chapitre 7 consacre autant d'attention à la structure des Sentinelles : la sécurité d'une blockchain PoS n'est jamais purement technique, elle est aussi — et peut-être surtout — une question de gouvernance humaine.

Verdict Attaque #1 :

Critère	Résultat
Coût théorique d'une capture initiale (réseau à ~100 validateurs)	De l'ordre de 1 million € (<i>estimation</i>), décroissant en risque à mesure que le réseau grandit vers l'objectif de 1000+ validateurs
Probabilité de succès	Faible mais non nulle au lancement ; en baisse continue avec la montée en charge du réseau
Détection	Quasi immédiate (divergence entre nœuds indépendants, alerte des observateurs)
Parade	Slashing automatique + réplication massive + réponse de gouvernance (hard fork)
Conclusion honnête	Une attaque coûteuse, auto-punitive et détectable — pas « impossible en pratique », mais un risque réel, géré, et qui diminue à mesure que le réseau de validateurs s'élargit et se diversifie

Nous assumons ce changement de conclusion par rapport à une version antérieure de cet argumentaire : prétendre à une impossibilité absolue aurait été plus confortable, mais faux. La vraie force du système n'est pas qu'il est inattaquable — aucun système ne l'est — c'est qu'une attaque y est chère, visible, punie automatiquement, et rattrapable collectivement.

ATTAQUE #2 : L'attaque DDoS (saturation du réseau)

Objectif de l'attaquant : surcharger les serveurs de millions de fausses requêtes pour empêcher les votes réels d'être enregistrés — par exemple, envoyer cent millions de votes bidon entre 19h et 20h pour bloquer le système au moment critique.

Pourquoi c'est gérable :

Parade 1 : la décentralisation. Le ShadowVote n'a pas un serveur central mais un réseau de nœuds répartis dans le monde (objectif 1000+, Chapitre 5). Pour saturer le système, il faudrait saturer simultanément les serveurs situés dans chaque pays hébergeant un nœud — une opération bien plus difficile que de faire tomber un serveur unique. Il faut cependant être honnête : lancer une attaque par saturation coûte aujourd'hui peu cher. La vraie défense est donc la répartition du réseau, combinée à des services professionnels de protection contre ce type d'attaque.

Parade 2 : la validation par signature. Chaque vote doit être signé avec une clé privée unique. Un attaquant qui veut envoyer cent millions de votes bidon a besoin de cent millions de clés privées valides — donc de cent millions d'inscriptions. Or l'inscription exige un email vérifié par code, une adresse IP plafonnée (un nombre limité d'inscriptions par IP), et un délai de carence avant de pouvoir voter. Créer massivement de faux comptes en un temps réduit devient donc extrêmement coûteux et lent.

Parade 3 : les pools de validation. Les votes ne sont pas validés un par un en temps réel : ils sont regroupés en pools (par paquets) toutes les quelques minutes. Si un pool contient une majorité de votes signés valides et une minorité de votes sans signature valide, seuls les premiers sont retenus — les faux votes sont rejetés automatiquement lors de la validation.

Verdict Attaque #2 :

Critère	Résultat
Coût	Élevé (centaines de milliers à quelques millions d'euros par heure, estimation sectorielle)
Impact	Ralentissement temporaire possible, sans perte de votes déjà validés
Détection	Immédiate
Parade	Décentralisation, signatures obligatoires, protections anti-DDoS standards (type Cloudflare, AWS Shield)
Conclusion	Attaque coûteuse et in fine inefficace sur le résultat du scrutin

ATTAQUE #3 : Le piratage de l'application mobile

Objectif de l'attaquant : infecter l'application d'un malware qui change secrètement le vote de l'utilisateur avant l'envoi — vous votez Candidat X, le virus bascule discrètement vers Candidat Y.

Pourquoi c'est détectable :

Parade 1 : le code open-source. Le code de l'application ShadowVote est public (dépôt ouvert). Grâce aux « compilations reproductibles », n'importe quel développeur peut vérifier que l'application distribuée correspond exactement au code source publié ; toute modification non autorisée devient détectable par la communauté qui l'audite.

Parade 2 : la vérification post-vote. Après avoir voté, vous recevez un reçu cryptographique. Vous pouvez, avec votre clé privée, interroger la blockchain pour vérifier que le vote enregistré sous votre identifiant correspond bien à votre choix. Si l'application a été compromise, l'écart est visible dès cette vérification — même si, nous le verrons en section 2, cette vérification a elle-même des limites face à la coercition.

Parade 3 : les signatures numériques. L'application officielle est signée numériquement par ses développeurs ; le système d'exploitation vérifie automatiquement cette signature avant l'installation. Une version modifiée sans autorisation est rejetée par le téléphone lui-même.

Verdict Attaque #3 :

Critère	Résultat
Coût	De l'ordre de 50 000 à 200 000 € pour développer un malware sophistiqué (<i>estimation</i>)
Probabilité de succès	Faible, en raison d'une détection rapide par la communauté et par l'utilisateur lui-même
Parade	Code open-source, signatures numériques, vérification post-vote
Conclusion	Risque réel mais limité, avec des mécanismes de détection multiples

ATTAQUE #4 : Le phishing (faux site web)

Objectif de l'attaquant : créer un faux site « ShadowVote » pour voler les clés privées des utilisateurs — un email frauduleux invitant à « vérifier votre vote » sur `shadowv0te.com` (un zéro à la place d'un O) en est l'illustration classique.

Pourquoi ça reste un risque, comme pour toute application en ligne.

Le phishing fonctionne toujours sur une partie des utilisateurs, quel que soit le service visé — c'est vrai pour les sites bancaires, pour impots.gouv.fr, pour PayPal. C'est structurellement le risque numéro un de toute application grand public, et il serait malhonnête de prétendre que le ShadowVote y échapperait par magie.

Parades, standards de l'industrie :

- **Communication officielle claire** : dès l'inscription, l'application rappelle l'adresse officielle unique et martèle qu'aucune clé privée ne doit jamais être communiquée à qui que ce soit, y compris à un prétendu support technique.
- **Double authentification (2FA)** : voter nécessite la clé privée *et* un code envoyé par SMS sur le téléphone enregistré. Un pirate qui vole uniquement la clé privée ne peut pas voter sans accès au second facteur.
- **Éducation des utilisateurs** : tutoriels, campagnes de sensibilisation, messages répétés dans l'application — « si quelqu'un vous demande votre clé privée, c'est une arnaque ».

Verdict Attaque #4 :

Critère	Résultat
Coût	De l'ordre de 5 000 à 20 000 € pour créer un faux site crédible (<i>estimation</i>)
Probabilité de succès	Une frange des utilisateurs (de l'ordre de quelques pour cent, comme pour tout service en ligne) peut se faire piéger
Parade	Éducation, 2FA obligatoire, HTTPS, communication officielle
Conclusion	Risque réel et structurel — comme pour les banques — mais gérable, et atténué par le second facteur d'authentification

ATTAQUE #5 : L'achat de votes

Objectif de l'attaquant : acheter des votes en masse — « je te donne 50 € si tu votes pour le Candidat Y, prouve-le-moi en me montrant ton reçu ».

Le mécanisme central : le reçu ne prouve rien à un tiers absent. Votre reçu de vote contient votre identifiant pseudonyme (le même qui apparaît, en clair, sur le registre public — nous y revenons en détail section 2) et votre vote. Mais ce reçu, sous forme d'image ou de capture d'écran, se falsifie en quelques minutes avec n'importe quel outil de retouche : rien

n'empêche un électeur de voter pour son propre candidat, puis de fabriquer un faux reçu affichant le candidat exigé par l'acheteur, de l'encaisser, et de garder son vote réel secret. L'acheteur ne peut jamais vérifier l'authenticité d'un reçu sans posséder la clé privée de l'électeur — ce qui rend l'achat de vote *a posteriori*, à distance, économiquement absurde : personne de rationnel ne paierait pour une preuve qu'il ne peut pas authentifier.

La limite honnête de cette parade — et il faut la dire clairement. Ce mécanisme protège contre un scénario précis : un acheteur absent au moment du vote, qui se contente d'exiger une preuve *après coup*. Il ne protège **pas** contre deux scénarios différents, que nous devons nommer plutôt que passer sous silence :

1. **La coercition en direct.** Rien n'empêche un employeur ou un proche malveillant d'exiger que l'électeur vote *en sa présence*, sur son propre écran, sous ses yeux. Aucun reçu falsifiable ne protège contre une supervision en temps réel — ce n'est pas une faiblesse propre au ShadowVote, c'est une limite structurelle de **tout vote effectué à distance et hors d'un isoloir contrôlé par l'État**, y compris le vote par correspondance déjà légal dans de nombreux pays. L'urne papier, elle, bénéficie d'une protection que le vote à distance ne peut pas reproduire : la loi impose la solitude physique dans l'isoloir, sous le contrôle d'assesseurs neutres. C'est un vrai avantage du bureau de vote traditionnel, et il serait malhonnête de le nier. 2. **La connaissance préalable de l'identifiant.** Un acheteur ou un coerciteur suffisamment organisé pourrait exiger de connaître l'identifiant public de l'électeur *avant* le scrutin, puis consulter lui-même le registre public une fois le vote clos — sans avoir besoin d'un reçu du tout. Ce scénario, plus sophistiqué, est traité en détail dans la section suivante, car il touche au cœur même du modèle d'anonymat du ShadowVote.

Une parade complémentaire : le revote. Comme plusieurs systèmes de vote électronique existants (le modèle estonien, notamment), le ShadowVote permet de revoter autant de fois que nécessaire jusqu'à la clôture du scrutin — seul le dernier vote enregistré est compté. Un électeur contraint de voter devant un tiers peut ainsi, une fois seul, annuler ce choix forcé en revotant en toute discrétion avant la fermeture des urnes numériques. Ce n'est pas une solution parfaite — elle suppose que l'électeur retrouve un moment de solitude avant la clôture — mais c'est une protection réelle qui n'existe pas avec un bulletin papier déjà glissé dans l'urne.

Comparaison avec l'urne papier. L'achat de vote classique — photographier son bulletin dans l'isoloir avant de le glisser dans l'urne — reste, en pratique, plus simple à mettre en œuvre à grande échelle qu'une fraude au ShadowVote reposant sur un reçu falsifiable, précisément parce que la preuve « photo du bulletin réel » est, elle, authentique et vérifiable

par l'acheteur. Le ShadowVote inverse ce rapport de force pour la corruption *a posteriori*, sans l'annuler pour la coercition *en direct*.

Verdict Attaque #5 :

ShadowVote plus résistant que l'urne papier contre l'achat de vote non supervisé et différé ; **pas plus résistant** — et sur ce point précis, structurellement moins protégé qu'un isolement physique — contre la coercition supervisée en temps réel.

Tableau comparatif de sécurité globale

Type d'attaque	Urne papier	ShadowVote (blockchain)
Bourrage d'urne	Possible (cas avérés)	Très difficile (signature unique par électeur)
Modification des résultats après coup	Possible (centralisation du dépouillement)	Très difficile (décentralisation, réplication)
Destruction de votes	Possible (incendie, vol)	Très difficile (copies multiples et indépendantes)
Erreur de comptage	Possible (facteur humain)	Quasi nulle (comptage automatique)
Capture d'une majorité de validateurs	Sans objet	Coûteuse, détectable, punie par slashing, rattrapable par gouvernance
Attaque DDoS	Impossible (pas de réseau)	Ralentissement temporaire possible, sans perte de votes
Phishing	Impossible (pas de canal numérique)	Risque réel, géré (comme pour les banques)
Achat de vote non supervisé	Possible (photo du bulletin)	Très difficile (reçu falsifiable)
Coercition en direct	Limitée par la loi (isolement obligatoire)	Risque réel, non résolu par la seule technique

Conclusion sécurité globale : le ShadowVote est supérieur ou équivalent à l'urne papier sur la majorité des critères techniques — bourrage, falsification *a posteriori*, erreurs de comptage — et lui reste inférieur sur un point précis et assumé : la garantie physique de solitude qu'offre un isolement surveillé par la loi. C'est un bilan solide, pas un bilan parfait.

2. Anonymat : une pseudonymisation forte, pas un secret absolu

La promesse — et sa vraie nature

« Personne, pas même l'État, ne doit savoir pour qui j'ai voté. » C'est le principe du secret du scrutin, inscrit dans la loi. Le ShadowVote respecte-t-il cette promesse ?

La réponse honnête est plus nuancée qu'un simple « oui » — et c'est précisément cette nuance que ce chapitre doit assumer plutôt que gommer, car elle a déjà été relevée, ailleurs dans le monde, par des chercheurs qui ne se sont pas laissé endormir par des affirmations rassurantes.

Ce que le ShadowVote garantit dès le lancement : une pseudonymisation forte. Pour tout observateur extérieur — un citoyen qui consulte le registre public, un journaliste, un candidat, un parti concurrent — il est cryptographiquement impossible de relier un identifiant de vote à une identité réelle sans information supplémentaire. C'est une garantie réelle et solide, comparable à celle qu'offre un bulletin sous enveloppe anonyme.

Ce que le ShadowVote ne garantit pas encore : un secret cryptographique absolu du contenu du vote. Le registre public affiche, en clair et de façon permanente, que « l'identifiant SV-FR-2027-8f3e7a... a voté Candidat X ». Ce lien identifiant → choix n'est jamais chiffré ni caché : il est public par construction, puisque c'est ce qui permet à chacun de vérifier l'intégrité du scrutin (Chapitre 5). La seule protection réside dans le fait de ne pas savoir qui se cache derrière cet identifiant. C'est une architecture différente — et objectivement plus faible sur ce point précis — que celle du bulletin papier, où même si l'on connaît l'identité d'un électeur, il est impossible de retrouver son choix a posteriori.

Et il y a plus : contrairement à ce qu'une lecture rapide pourrait laisser penser, l'opérateur technique du système **n'est pas dans l'impossibilité absolue** de faire le lien entre un identifiant et une personne réelle. L'inscription requiert un email vérifié, une adresse IP enregistrée à des fins anti-fraude, et un numéro de téléphone pour la double authentification par SMS. Ces informations sont conservées, quelque part, dans les systèmes d'inscription — même si elles ne transitent jamais vers la blockchain elle-même. Un opérateur malveillant, un pirate ayant compromis la base d'inscription, ou une autorité disposant d'un pouvoir de réquisition légal pourrait donc, en théorie, croiser ces données et retrouver l'identité derrière un identifiant. Prétendre le contraire, comme le faisait une version antérieure de cet argumentaire, serait à la fois inexact et dangereux : un

système qui peut techniquement relier vote et identité doit être présenté comme tel, et pas comme offrant une impossibilité absolue.

C'est très précisément la raison pour laquelle le Chapitre 7 consacre une gouvernance entière à ce problème : le ShadowVote n'a pas vocation à être opéré par une seule entité centrale disposant d'un accès unilatéral à toutes ces données. Il repose sur une gouvernance décentralisée entre plusieurs institutions indépendantes (les Sentinelles et leurs partenaires), avec séparation des rôles, chiffrement à garde partagée (aucune entité seule ne détient la clé complète permettant de croiser inscription et vote), purge des journaux de connexion une fois l'éligibilité vérifiée, et obligation d'une décision judiciaire multipartite pour toute levée exceptionnelle de cette séparation. La garantie de fond n'est donc pas seulement cryptographique : elle est aussi organisationnelle et politique. C'est une différence de nature avec l'urne papier, où le secret repose sur un mécanisme physique simple (l'isoloir, l'enveloppe, l'urne scellée) ; ici, le secret repose sur une architecture de confiance distribuée, qui doit être gouvernée avec la même rigueur que la cryptographie elle-même.

Encadré — ce que le ShadowVote garantit, et ce qu'il ne garantit pas encore

	Aujourd'hui (lancement)	À terme (feuille de route)
Séparation identité / identifiant public	Oui — pseudonymisation cryptographique forte	Inchangé
Secret du contenu du vote face à un observateur extérieur	Oui, tant que l'identifiant n'est pas relié à une personne	Oui, quel que soit qui consulte le registre (via preuves à divulgation nulle de connaissance, voir plus bas)
Impossibilité pour l'opérateur de relier vote et identité	Non — techniquement possible, contenue par la gouvernance décentralisée (Chapitre 7) et la purge des journaux	Objectif : rendre ce lien mathématiquement impossible, pas seulement organisationnellement contenu
Résistance à l'achat de vote a posteriori	Oui (reçu falsifiable)	Inchangé
Résistance à la coercition en temps réel	Non résolue par la technique seule	Limitée structurellement, comme pour tout vote

		à distance
--	--	------------

Le pseudonymat cryptographique expliqué

Étape 1 : vous créez votre identité numérique. Lors de l'inscription, l'application génère un identifiant public (par exemple `SV-FR-2027-8f3e7a2d9c1b5e4f6a8d3c7b2e1f9a4c`) et une clé privée que vous seul détenez. L'identifiant public fonctionne comme une boîte aux lettres : tout le monde peut voir qu'elle existe et qu'elle reçoit du courrier, mais seule la clé privée — la clé de la boîte — permet d'en lire le contenu ou de prouver qu'on en est le titulaire.

L'application ne demande ni votre nom, ni votre adresse, ni votre numéro de sécurité sociale, ni une pièce d'identité scannée. Elle demande en revanche, pour des raisons de sécurité anti-fraude détaillées en section 1, un email vérifié, une adresse IP à l'inscription, et un numéro de téléphone pour le second facteur d'authentification — c'est précisément ce triptyque qui, conservé côté opérateur, constitue le vecteur théorique de désanonymisation évoqué plus haut, et que la gouvernance du Chapitre 7 a vocation à encadrer.

Étape 2 : vous votez. Votre vote est enregistré dans la blockchain sous une forme simple :

```
```json {  "identifiant": "SV-FR-2027-8f3e7a2d...",  "vote": "CandidatX",  "timestamp": "2027-04-18T10:24:03Z" } ```
```

Ce que tout observateur voit sur le registre public	Ce qu'il ne peut pas déduire sans information supplémentaire
L'identifiant `SV-FR-2027-8f3e7a...` a voté pour X	Qui est cette personne dans la vraie vie

**Étape 3 : vous vérifiez, vous et vous seul.** Avec votre clé privée, vous pouvez interroger la blockchain et confirmer que le vote enregistré sous votre identifiant correspond bien à votre choix. Personne d'autre ne peut faire cette vérification à votre place, faute de détenir votre clé — mais rappelons, comme nous l'avons vu section 1, que cette même vérification peut être détournée par un tiers qui exigerait de la faire *avec vous*, sous contrainte.

## Les garanties techniques, et leurs limites assumées

**Garantie 1 — séparation identité/vote.** À l'urne, vous signez la liste d'émargement (votre identité) puis vous glissez le bulletin (votre vote) : une séparation physique. Au ShadowVote, vous créez un identifiant pseudonyme puis vous votez avec cet identifiant : une séparation cryptographique. Le principe est équivalent ; la robustesse pratique dépend, on l'a vu, de la gouvernance qui encadre les données d'inscription.

**Garantie 2 — l'irréversibilité du hachage.** L'identifiant est dérivé par un algorithme de hachage cryptographique (SHA-256), une fonction à sens unique : facile à calculer dans un sens (données → hash), impossible à inverser dans l'autre (hash → données), à l'image d'un gâteau qu'on ne peut pas déconstruire pour retrouver la farine, les œufs et le sucre d'origine. Casser un hash SHA-256 par force brute exigerait de tester  $2^{256}$  combinaisons — un nombre si vaste qu'aucun ordinateur existant, ni prévisible, n'y parviendrait avant des durées dépassant l'âge de l'univers. C'est une garantie mathématique solide : elle protège contre la reconstruction de l'identifiant à partir du hash, mais elle ne protège pas — nous insistons — contre le simple fait que l'opérateur connaisse déjà, par ailleurs, la correspondance entre votre email et votre identifiant, puisqu'il l'a générée lui-même à l'inscription.

**Garantie 3 — ce qui n'est pas transmis à la blockchain.** L'application voit effectivement votre adresse IP, votre type d'appareil, et potentiellement votre localisation approximative. Mais ces données ne sont jamais envoyées à la blockchain : seuls l'identifiant, le vote et la signature y sont inscrits. Voter via un VPN peut renforcer cette protection en masquant votre adresse IP réelle même vis-à-vis de l'application elle-même. Cette garantie est réelle mais partielle : elle protège la blockchain publique, pas nécessairement les journaux internes du système d'inscription, dont la sécurité et la politique de purge relèvent, encore une fois, de la gouvernance décrite au Chapitre 7.

**Garantie 4 — le vecteur du registre public et de l'identifiant connu à l'avance.** C'est le point le plus délicat, et celui qu'un chapitre honnête ne peut pas éluder. Puisque le registre affiche en clair « identifiant X a voté Y », toute personne qui parviendrait à connaître à l'avance votre identifiant — parce que vous le lui avez montré, parce qu'il a été intercepté, ou parce qu'un opérateur compromis l'a communiqué — pourrait ensuite consulter elle-même le résultat associé, sans avoir besoin de vous croire sur parole ni de vous demander un reçu. Les parades à ce scénario ne sont pas purement techniques : identifiant renouvelé à chaque scrutin plutôt que réutilisé d'une élection à l'autre (pour limiter le profilage dans le temps), sensibilisation explicite des électeurs à ne jamais communiquer leur identifiant avant la clôture du vote, et surtout, cadre légal rappelant que solliciter la divulgation préalable d'un identifiant de vote à des fins de contrôle constitue une infraction assimilable à la corruption électorale, quel que soit le support du scrutin.

**Garantie 5 — la coercition, reprise et complétée.** Nous avons détaillé en section 1 (Attaque #5) le mécanisme du reçu falsifiable et sa limite face à une supervision en direct. Ajoutons ici l'élément propre à l'anonymat : même en l'absence de supervision directe, un acheteur de vote qui aurait obtenu votre identifiant *avant* le scrutin — par le vecteur décrit au paragraphe précédent — n'a pas besoin de votre reçu du tout. C'est pourquoi la protection contre la coercition ne peut pas reposer sur la seule

fabrication d'un faux reçu : elle repose sur la combinaison de plusieurs mesures — reçu non vérifiable par un tiers absent, possibilité de revoter jusqu'à la clôture, non-divulgateur de l'identifiant avant le vote, et sanction légale de toute tentative de contrôle du choix électoral.

## Les Zero-Knowledge Proofs : la vraie trajectoire vers le secret absolu

Les preuves à divulgation nulle de connaissance (*Zero-Knowledge Proofs*, ZKP) sont des algorithmes cryptographiques permettant de prouver qu'une affirmation est vraie sans révéler l'information elle-même. L'exemple classique : prouver que vous avez plus de 18 ans sans révéler votre âge exact, votre adresse ou votre photo — le vérifieur apprend seulement que la condition est remplie, rien de plus.

Appliquées au vote, les ZKP permettraient de prouver qu'un électeur a voté, et que son vote a été correctement comptabilisé dans le résultat final, **sans jamais révéler pour qui**, y compris sur le registre public consulté par n'importe qui. C'est la différence de nature entre la pseudonymisation d'aujourd'hui (le lien identifiant → choix est public, seule l'identité de la personne derrière l'identifiant est protégée) et le secret cryptographique visé à terme (même le lien identifiant → choix disparaît du registre, remplacé par une preuve mathématique globale d'intégrité).

Nous ne prétendons pas que cette technologie équipe le ShadowVote dès son lancement : elle est aujourd'hui complexe à mettre en œuvre à l'échelle de millions d'électeurs et coûteuse en calcul. C'est une évolution de la feuille de route, pas une fonctionnalité déjà livrée — et c'est précisément pourquoi ce chapitre distingue, depuis le début de cette section, ce qui est acquis (le pseudonymat) de ce qui reste à construire (le secret cryptographique total). Présenter les deux comme équivalents aurait été la faille la plus immédiatement exploitable de tout cet argumentaire face à un lecteur technique.

## Comparaison anonymat : urne papier vs ShadowVote

Critère	Urne papier	ShadowVote (aujourd'hui)
Séparation identité/vote	Oui (physique)	Oui (cryptographique, pseudonymisation forte)
Secret du contenu du vote même si l'identité de l'électeur est connue	Oui, absolu	Non — le lien identifiant/choix est public ; seule l'identité derrière l'identifiant est protégée
Risque de lien par	Sans objet	Techniquement

l'opérateur du système		possible, contenu par la gouvernance décentralisée (Chapitre 7)
Protection IP/localisation	Sans objet (non numérique)	Oui pour la blockchain publique ; dépend des journaux d'inscription pour le reste
Résistance à l'achat de vote non supervisé	Faible (photo du bulletin)	Forte (reçu non vérifiable par un tiers absent)
Résistance à la coercition en direct	Bonne (isoloir garanti par la loi)	Limitée — comme tout vote à distance
Trajectoire d'amélioration	Aucune (mécanisme figé)	Preuves à divulgation nulle de connaissance (ZKP), à terme

**Conclusion anonymat :** le ShadowVote offre une pseudonymisation forte, robuste contre l'essentiel des usages malveillants classiques — profilage de masse, revente de listes, corrélation commerciale, identification par un observateur extérieur — et une résistance réelle et nouvelle à l'achat de vote non supervisé. Ce n'est pas, en revanche, un secret cryptographique absolu comparable à celui de l'isoloir sur deux points précis : la théorique capacité de l'opérateur à faire le lien entre identité et vote, et la vulnérabilité à la coercition en temps réel. La réponse à ces deux limites n'est pas seulement technique : elle est fondamentalement une question de gouvernance — ce qui explique pourquoi le Chapitre 7, consacré aux Sentinelles, n'est pas un simple prolongement organisationnel de ce chapitre, mais sa condition de validité.

---

### 3. Accessibilité : de 7 à 107 ans

#### La question qui tue (bis)

« OK, c'est génial pour les jeunes qui ont un smartphone. Mais ma grand-mère de 87 ans, qui sait à peine envoyer un SMS, comment elle fait ? »

Réponse : elle a le choix.

- **Option 1 — elle vote juste à l'urne, comme d'habitude.** Le ShadowVote n'est pas obligatoire. Il se présente comme un vote parallèle citoyen (Chapitres 5 et 9), pas comme un remplacement forcé : l'urne reste disponible pour tous, sans exception, aussi longtemps que le système officiel existera.

- **Option 2 — elle se fait aider.** Comme pour une carte bancaire, un proche peut l'accompagner dans les étapes techniques, sans jamais voir son vote final.
- **Option 3 — une interface ultra-simplifiée.** L'application propose un mode « senior » à trois boutons géants, pensé pour minimiser la charge cognitive.

## **Les cinq niveaux d'accessibilité**

**Niveau 1 — les technophiles (20-40 ans).** Profil : Yanis, 31 ans, développeur. Il télécharge l'application en dix secondes, crée son identifiant en trente secondes, vote en vingt secondes, vérifie en dix secondes. Temps total : environ soixante-dix secondes.

**Niveau 2 — les utilisateurs moyens (40-60 ans).** Profil : Sophie, 42 ans, professeure. Elle suit un tutoriel vidéo de trois minutes, télécharge l'application avec l'aide du store, puis vote guidée étape par étape grâce à une interface claire. Temps total : environ cinq minutes.

**Niveau 3 — les seniors autonomes (60-75 ans).** Profil : Jean, 68 ans, retraité. Il assiste à un atelier d'initiation organisé en mairie, à la bibliothèque ou dans une association ; il télécharge l'application avec l'aide d'un bénévole, puis vote grâce au mode « senior » (gros boutons, texte agrandi). Temps total : environ quinze minutes, après une heure de formation préalable.

**Niveau 4 — les seniors assistés (75-90 ans).** Profil : Odette, 82 ans, retraitée. Sa petite-fille installe l'application sur sa tablette et configure le compte avec son accord — sans jamais voir le vote final, qui reste strictement personnel. Odette vote ensuite seule, en trois clics, grâce à une interface ultra-simplifiée. Temps total : environ deux minutes, après une installation assistée en amont.

**Niveau 5 — les personnes en situation de handicap.** Profil : Bruno, 45 ans, malvoyant. Il utilise le mode accessibilité, compatible avec les lecteurs d'écran natifs (VoiceOver sur iOS, TalkBack sur Android), vote par commande vocale et reçoit une confirmation audio. Temps total : environ deux minutes. Une précaution mérite d'être ajoutée ici, et le livre aurait tort de la taire : voter à voix haute, comme le permet ce mode audio, peut casser le secret du vote si l'électeur n'est pas seul au moment de l'interaction — l'usage d'un casque ou d'écouteurs est donc recommandé, au même titre qu'un accompagnement discret pour s'assurer que l'électeur vote hors de portée d'oreilles indiscretes.

## **L'interface en trois écrans**

### **Écran 1 — Accueil.**



## Comparaison accessibilité : urne papier vs ShadowVote

Critère	Urne papier	ShadowVote
Personnes valides	Facile	Facile
Seniors autonomes	Facile	Formation nécessaire (environ une heure)
Seniors assistés	Aidé par un assesseur	Aidé par un proche, sans qu'il voie le vote final
Handicap moteur	Accès au bureau de vote parfois difficile	Vote possible depuis chez soi
Malvoyants	Bulletin tactile, rare	Mode audio intégré (avec précaution d'usage en présence d'un tiers)
Sourds	Pas d'impact	Pas d'impact
Difficultés de lecture	Difficulté réelle	Mode photo et audio
Personnes isolées	Déplacement obligatoire	Vote possible depuis chez soi

**Conclusion accessibilité :** le ShadowVote est nettement supérieur pour certains publics — handicap moteur, isolement géographique — et nécessite, en contrepartie, un effort de formation réel pour les publics seniors les moins familiers du numérique. Ce n'est pas un gain uniforme : c'est un déplacement du curseur, qu'il faut accompagner d'investissements concrets (ateliers, hotline, aide à distance) plutôt que de présenter comme acquis sans effort.

---

## 4. Le coût réel

**Précision importante, avant les chiffres.** Tant que le ShadowVote reste un vote parallèle citoyen, il ne remplace pas l'urne : il s'y ajoute. Il ne fait donc économiser aucun argent public. La question honnête n'est pas « combien l'État économiserait-il ? », mais « combien coûterait la vérification citoyenne, comparée au prix d'une élection ? ».

### Ce que coûte une élection, ce que coûterait la vérification

**Organisation officielle (chiffres du Sénat) :**

Poste	Montant
Présidentielle et législatives de 2012	432 millions €
Moyenne par scrutin national	≈ 216 millions €

Par électeur inscrit et par scrutin (≈ 46 millions d'inscrits en 2012)	≈ 4,70 €
---------------------------------------------------------------------------	----------

*Source : rapport d'information d'Hervé Marseille au nom de la commission des finances du Sénat (octobre 2015). Ce coût comprend notamment la propagande électorale et le remboursement des dépenses de campagne.*

### **ShadowVote, à pleine échelle (estimation de l'auteur) :**

Poste	Coût par électeur
Transaction blockchain (réseau ShadowVote)	0,001 €
Infrastructure serveurs (amortie)	0,01 €
Support utilisateur	0,02 €
Maintenance logicielle	0,01 €
<b>Total</b>	<b>0,04 € par électeur, soit environ 2 millions € pour 50 millions d'inscrits</b>

Soit, à pleine échelle, moins de 1 % du coût d'un scrutin national — un ordre de grandeur, pas une promesse comptable.

### **Mais attendez : le coût de développement initial**

Ajoutons le développement initial et le fonctionnement annuel, sur dix ans — soit deux présidentielles et deux législatives, sans compter les scrutins locaux et européens :

- **Organisation officielle** : quatre scrutins nationaux × ≈ 216 millions € ≈ 860 millions €, hors élections locales et européennes.
- **ShadowVote** :

Poste	Coût
Développement et test pilote	≈ 0,8 à 1 million €
Fonctionnement annuel (10 × 700 000 €)	≈ 7 millions €
Coût direct des scrutins vérifiés (≈ 2 M€ par scrutin national)	≈ 8 millions €
<b>Total sur 10 ans (estimation)</b>	<b>environ 16 millions €</b>

Sur dix ans, la vérification citoyenne coûterait donc de l'ordre de 2 % du prix des seuls scrutins nationaux. Rappelons-le : ce n'est pas une économie, puisque l'urne reste en place. C'est le prix, modeste, de la preuve.

### **Et si l'État l'adoptait un jour ?**

Si, à long terme, l'État décidait d'intégrer officiellement un dispositif de ce type, certaines dépenses pourraient diminuer (impression, logistique, dépouillement). Mais une grande partie du coût d'une élection — la

propagande, le remboursement des campagnes, l'urne qui doit rester accessible à tous — ne disparaîtrait pas. Toute promesse d'économie massive serait donc imprudente.

Le choix de l'affectation d'éventuelles économies relèverait, le moment venu, d'un débat démocratique — pas de ce livre.

---

## Conclusion du chapitre : la plupart des objections techniques trouvent une réponse solide

Vous avez maintenant des réponses argumentées aux quatre objections centrales :

- **Sécurité** : un système plus robuste que l'urne papier sur la plupart des critères, avec une limite assumée — la solitude garantie par la loi dans l'isoloir n'a pas d'équivalent parfait dans un vote à distance.
- **Anonymat** : une pseudonymisation cryptographique forte, comparable au bulletin traditionnel sur l'essentiel des usages, avec une nuance technique importante — le lien entre identité et vote n'est pas mathématiquement impossible, il est contenu par une gouvernance décentralisée, et les preuves à divulgation nulle de connaissance en sont l'horizon d'amélioration.
- **Accessibilité** : un système utilisable de 7 à 107 ans, à condition d'investir réellement dans la formation, l'accompagnement et les dispositifs d'aide.
- **Coût** : un coût marginal — moins de 1 % du prix d'un scrutin national —, qui ne fait pas économiser d'argent tant que l'urne reste en place.

Il ne reste donc pas « aucune excuse technique », comme on pourrait être tenté de le proclamer trop vite : il reste des limites réelles, nommées, et des réponses qui relèvent autant de la gouvernance humaine (Chapitre 7) que de la seule cryptographie. C'est une différence importante — et c'est elle qui rend cet argumentaire plus solide, pas plus faible, face à l'examen critique.

## Bilan de la Partie II

Nous avons terminé la Partie II : la solution. Vous savez désormais ce qu'est la blockchain (Chapitre 4), comment fonctionne le ShadowVote (Chapitre 5), et dans quelle mesure il est sûr, pseudonymisé, accessible et économiquement soutenable — avec ses forces et ses limites assumées (Chapitre 6).

**Transition vers la Partie III.** Dans la partie suivante, nous verrons comment le ShadowVote peut devenir un mouvement : comment passer de l'outil technique à la mobilisation citoyenne, comment le déployer par

étapes, comment convaincre sans exagérer, et comment la gouvernance des Sentinelles, évoquée à plusieurs reprises dans ce chapitre, prend concrètement forme. La solution existe, avec ses limites. Il reste à la faire vivre, avec la même honnêteté.

# CHAPITRE 7

## LA DÉMOCRATIE DE L'OMBRE

*« Le pouvoir ne se prend pas. Il se retire. » — comme le veut l'adage*

### **Introduction : de l'outil au mouvement**

Nous avons posé le diagnostic (Partie I) : le système électoral est opaque et obsolète. Nous avons proposé la solution (Partie II) : le ShadowVote, une blockchain pour vérifier nos votes. Mais un outil, seul, ne suffit pas.

Un marteau ne construit pas une maison. Il faut un architecte, des ouvriers, un plan. Le ShadowVote est le marteau. La Démocratie de l'Ombre est le mouvement qui va construire la maison.

Ce chapitre pose les fondations philosophiques et stratégiques de ce mouvement. Qu'est-ce que la Démocratie de l'Ombre ? Pourquoi choisir le retrait stratégique plutôt que la confrontation ? Qui sont les Sentinelles ? En quoi ce mouvement se différencie-t-il de tous ceux qui l'ont précédé ?

À la fin de ce chapitre, vous comprendrez que le ShadowVote n'est pas qu'une application. C'est une philosophie d'action.

### **1. La Démocratie de l'Ombre : définition**

#### **Le concept central**

La Démocratie de l'Ombre n'est pas une démocratie cachée ni clandestine. C'est une démocratie parallèle — transparente et vérifiable — qui s'établit à côté du système officiel pour le surveiller, l'auditer et, à terme, le rendre obsolète.

#### **Une métaphore théâtrale**

Imaginez un théâtre. Le système officiel, c'est la scène principale. La Démocratie de l'Ombre, ce sont les spectateurs, jumelles en main, qui vérifient que les acteurs respectent le script. Les acteurs — l'État — savent qu'ils sont observés. Ils peuvent continuer à jouer. Mais ils ne peuvent plus tricher.

#### **Les trois piliers**

##### *Pilier 1 : de la délégation passive à la responsabilité active*

Le système actuel repose sur une délégation passive : vous votez, vous déléguez votre souveraineté à un élu, vous attendez cinq ans, vous espérez qu'il fait bien son travail — et vous n'avez aucun moyen de vérifier. C'est une foi aveugle.

La Démocratie de l'Ombre propose une responsabilité active : vous votez deux fois — dans l'urne et sur la blockchain. Vous déléguez, mais vous gardez une preuve. Vous vérifiez en temps réel que votre vote compte. Vous auditez les résultats publiquement. Vous disposez enfin d'un levier de contrôle permanent. C'est une vigilance documentée.

Système actuel	Démocratie de l'Ombre
Vous êtes un sujet qui obéit	Vous êtes un citoyen qui surveille
Le pouvoir vous est confisqué après le vote	Vous conservez le pouvoir sous forme de preuve
Foi aveugle en l'institution	Vigilance documentée et permanente

### *Pilier 2 : le retrait stratégique*

La méthode classique est celle de la confrontation : « Le système est pourri ! Manifestons ! Cassons ! Renversons ! » Son résultat historique est connu : répression, épuisement, échec (voir le Chapitre 3 sur les Gilets Jaunes).

La méthode de l'Ombre est celle du retrait stratégique : « Le système est opaque ? Nous créons notre propre système de vérification. Transparent. Public. Vérifiable. Nous n'attendons plus rien de l'État. Nous construisons à côté. » Le résultat attendu n'est pas l'affrontement, mais l'obsolescence progressive : le système officiel devient moins fiable que le système parallèle, jusqu'à ne plus pouvoir prétendre au monopole de la confiance.

### *Analogie : Uber contre les taxis*

Les chauffeurs de taxi ont manifesté contre Uber. Ils ont brûlé des pneus, bloqué des aéroports. Résultat : Uber a continué de croître. Pourquoi ? Parce qu'Uber ne s'est pas battu contre les taxis — Uber a construit un service meilleur. Les clients ont choisi. Le marché a tranché. Les taxis ont dû s'adapter ou disparaître.

Le ShadowVote applique la même logique au vote. Nous ne nous battons pas contre l'urne. Nous construisons un système meilleur que l'urne. Les citoyens choisiront. L'histoire tranchera. L'État devra s'adapter.

### *Pilier 3 : la preuve comme arme non-violente*

Type de mobilisation	Méthode	Résultat
Violence physique	Cailloux, cocktails Molotov	Répression, arrestations, échec moral
Violence symbolique	Grèves, blocages, occupations	Lassitude, perte de sympathie, échec stratégique
Preuve	Code inaltérable,	Difficile à réprimer,

cryptographique	registre public	difficile à discréditer
-----------------	-----------------	-------------------------

La preuve est l'arme parfaite. Elle ne blesse personne. Elle ne détruit rien. Elle est difficile à censurer, grâce à la décentralisation. Elle est très difficile à falsifier, grâce à la blockchain. Elle est difficile à ignorer, grâce à la pression morale qu'elle exerce. Le Code ne crie pas. Il démontre.

### **Pourquoi « de l'Ombre » ?**

Ce n'est pas une ombre sinistre. C'est l'ombre du doute que nous projetons sur le système officiel. Quand les résultats du ShadowVote divergent de ceux de l'urne, nous créons une zone d'ombre sur la légitimité du scrutin. L'État doit alors sortir de l'ombre et prouver qu'il a raison.

C'est une inversion de la charge de la preuve. Aujourd'hui, c'est au citoyen de prouver qu'il y a fraude. Demain, ce sera à l'État de prouver qu'il n'y en a pas.

## **2. Le pouvoir du retrait stratégique**

### **L'histoire nous enseigne**

Les mouvements qui ont changé le monde n'ont pas toujours vaincu par la force. Souvent, ils ont vaincu par le retrait du consentement. Trois exemples historiques l'illustrent.

#### *Exemple 1 : Gandhi et la Marche du sel (1930)*

L'Inde est alors colonisée par l'Empire britannique, qui détient le monopole de la production de sel : les Indiens doivent acheter le sel anglais et en payer la taxe. La confrontation classique aurait pu prendre la forme d'une révolte armée, d'attaques des postes de douane, d'une guerre d'indépendance violente.

Gandhi a choisi autre chose. Il a marché jusqu'à la mer, ramassé du sel de ses propres mains, et cassé ainsi le monopole britannique en produisant son propre sel. Un acte simple. Non-violent. Symbolique. Des milliers d'Indiens l'ont imité, produisant leur propre sel et refusant d'acheter le sel anglais. Le monopole ne tombe pas du jour au lendemain — la taxe sur le sel ne sera abolie qu'à la veille de l'indépendance —, mais dès 1931, le pacte Gandhi-Irwin autorise les habitants des côtes à produire leur propre sel. Une brèche ouverte non par la violence, mais par le retrait du consentement.

Le ShadowVote est notre Marche du sel. L'État détient le monopole de la validation électorale. Nous créons notre propre système de validation. Nous cassons le monopole.

#### *Exemple 2 : la chute du Mur de Berlin (1989)*

En Allemagne de l'Est, sous dictature communiste et surveillance totale de la Stasi, la confrontation classique aurait pu prendre la forme d'une révolte armée, d'une guerre civile, d'un bain de sang.

Ce qui s'est réellement passé : les citoyens est-allemands ont massivement demandé des visas pour l'Ouest et manifesté pacifiquement, scandant « Wir sind das Volk » (Nous sommes le peuple). Le 9 novembre 1989, à la suite d'une annonce confuse d'un porte-parole du régime, des milliers de citoyens se sont précipités vers le Mur ; les gardes-frontières, dépassés, les ont laissés passer. Le Mur est tombé — non par la violence, mais par le retrait massif du consentement.

Le ShadowVote vise un effet comparable. Quand une part significative des électeurs utilise le ShadowVote et que les résultats divergent de ceux de l'urne, le système officiel perd en légitimité, ses gardiens — élus, hauts fonctionnaires de l'opacité — sont dépassés, et le mur de l'opacité finit par tomber.

### *Exemple 3 : le boycott des bus de Montgomery (1955-1956)*

En Alabama, la ségrégation raciale impose aux Noirs de s'asseoir à l'arrière des bus. Rosa Parks refuse de céder sa place à un passager blanc ; elle est arrêtée. La confrontation classique aurait pu prendre la forme d'émeutes, de violences, de répression.

Ce que Martin Luther King a organisé fut tout autre : un boycott total des bus, pendant 381 jours. Les Noirs de Montgomery marchent à pied, s'organisent en covoiturage, refusent de payer le bus. La compagnie perd une part considérable de ses revenus. En novembre 1956, la Cour suprême des États-Unis confirme que la ségrégation dans les bus est inconstitutionnelle (arrêt *Browder v. Gayle*) — une victoire obtenue non par la violence, mais par la combinaison du retrait économique et du droit.

Le ShadowVote organise un boycott symbolique comparable. Nous ne boycottons pas l'urne — nous y allons toujours. Nous boycottons la confiance aveugle. Nous disons : « Je vote dans votre urne, mais je ne vous fais plus confiance. Je vérifie moi-même. »

### **La leçon stratégique**

Ces trois exemples ont un point commun : le pouvoir ne se prend pas, il se retire. Quand suffisamment de citoyens retirent leur consentement — leur confiance, leur argent, leur participation aveugle — le système s'effondre. Le ShadowVote est un retrait du consentement à l'opacité.

Ces trois cas sont des succès reconnus ; d'autres tentatives de retrait, dans d'autres contextes, ont échoué ou ont mis des décennies à porter leurs fruits. Le retrait stratégique n'est pas une formule magique : c'est une méthode qui exige du nombre, de la durée et de la discipline non-violente. C'est précisément ce que la Démocratie de l'Ombre entend organiser.

## **Pourquoi le retrait fonctionne mieux que la confrontation**

*Raison 1 : le système ne peut pas réprimer ce qui ne l'attaque pas.* Une manifestation violente ? L'État envoie la police. Une grève illimitée ? L'État réquisitionne. Un vote parallèle, légal et transparent ? L'État se trouve démuni : rien ne l'empêche juridiquement d'encadrer, voire de contester un tel système au nom de l'ordre public ou du secret du vote — mais interdire purement et simplement une démarche de vérification citoyenne reviendrait à admettre publiquement que cette vérification le menace. C'est un aveu qu'aucun pouvoir ne peut se permettre facilement.

*Raison 2 : le retrait préserve l'énergie citoyenne.* Manifester pendant des mois épuise. Vérifier son vote prend quelques minutes. Coût énergétique minimal, impact potentiellement maximal.

*Raison 3 : le retrait gagne par l'évidence.* Vous n'avez pas à convaincre l'État de se réformer. Vous n'avez qu'à convaincre les citoyens de vérifier. Si une minorité vérifie et que les résultats divergent, la majorité voudra vérifier à son tour. La contagion devient alors quasi automatique.

## **3. Les Sentinelles : gardiens de la preuve**

### **Qui sont les Sentinelles ?**

Les Sentinelles sont les citoyens qui utilisent le ShadowVote. Ce n'est pas un parti politique. Ce n'est pas une organisation hiérarchique. Ce n'est pas un mouvement avec un leader. C'est un réseau horizontal de citoyens vigilants.

### **Le rôle d'une Sentinelle**

*Action 1 — voter deux fois.* Le dimanche du scrutin : voter dans l'urne (le vote officiel), puis voter sur la blockchain (le vote témoin). Temps nécessaire : deux minutes.

*Action 2 — vérifier.* Le soir, à vingt heures : consulter les résultats ShadowVote, les comparer aux résultats officiels, vérifier que son propre vote est bien enregistré. Temps nécessaire : cinq minutes.

*Action 3 — alerter.* En cas de divergence détectée : partager sur les réseaux sociaux, alerter les médias, informer d'autres Sentinelles. Temps nécessaire : dix minutes.

Le bilan : dix-sept minutes pour protéger la démocratie. C'est moins de temps que pour regarder un épisode de série.

### **Le serment de la Sentinelle**

Les Sentinelles n'ont pas de chef. Elles n'ont pas de carte de membre. Elles n'ont pas de cotisation. Elles ont un serment moral :

**JE M'ENGAGE À VÉRIFIER.**

Je ne crois plus sans preuve.

Je ne délègue plus sans contrôle.

Je ne vote plus sans témoin.

Je suis une Sentinelle.

Je garde la preuve.

Je surveille les élections.

Non par défiance systématique,  
mais par responsabilité citoyenne.

Si le système converge, je le valide.

Si le système diverge, je l'alerte.

Plus jamais sans preuve.

Ce serment n'est pas religieux : c'est un engagement civique. Comme le serment du médecin (« Primum non nocere » — d'abord ne pas nuire). Comme le serment du pompier (« Sauver ou périr »). Le serment de la Sentinelle pourrait se résumer ainsi : « Vérifier ou subir. »

### **Les trois types de Sentinelles**

*Type 1 — la Sentinelle passive (la majorité).* Sophie, 42 ans, professeure. Elle utilise le ShadowVote pour ses propres élections, vérifie son vote, mais ne milite pas activement. Son rôle : augmenter le nombre de votes ShadowVote, c'est-à-dire bâtir la masse critique. Quand des millions de citoyens comme elle utilisent le ShadowVote, la pression morale devient réelle.

*Type 2 — la Sentinelle active (les convaincus).* Elias, 31 ans, développeur. Il utilise le ShadowVote, en parle autour de lui, partage sur les réseaux sociaux, et anime un atelier d'initiation dans sa ville. Son rôle : propager le mouvement — une forme d'évangélisation civique.

Voici comment cette propagation peut, en théorie, se déployer par générations successives. Admettons qu'une Sentinelle active convainque en moyenne dix personnes de la rejoindre à leur tour comme Sentinelles actives : à la génération 1, une Sentinelle active en forme dix ; à la génération 2, ces dix en forment chacune dix, soit cent ; à la génération 3, ces cent en forment chacune dix, soit mille ; à la génération 4, ces mille en forment chacune dix, soit dix mille Sentinelles actives cumulées. Si chacune de ces dix mille Sentinelles actives convainc à son tour dix Sentinelles

passives, cela porte le mouvement à cent mille Sentinelles passives supplémentaires. Ce schéma est une simplification pédagogique : dans la réalité, les taux de conversion varient et ne sont jamais parfaitement réguliers. Mais le principe qu'il illustre est celui de tous les phénomènes de diffusion virale : une croissance qui semble négligeable au départ devient, palier après palier, difficile à arrêter.

*Type 3 — la Sentinelle contributrice (les bâtisseurs).* Marie, 38 ans, développeuse blockchain. Elle utilise le ShadowVote, contribue au code en open-source, héberge un nœud de validation, finance le projet (un don de 100 €) et participe à la gouvernance. Son rôle : construire et maintenir l'infrastructure. Quand une centaine de contributrices et contributeurs de ce type s'engagent, le système devient résilient, décentralisé, autonome.

Tous les types sont essentiels. Il n'y a pas de hiérarchie, pas de « meilleure » Sentinelle : chacune contribue à sa mesure.

### **Pourquoi « Sentinelles » ?**

Une sentinelle, c'est un gardien vigilant. Dans l'armée, elle monte la garde, surveille, alerte en cas de danger, ne dort jamais. Les Sentinelles de la Démocratie de l'Ombre montent la garde citoyenne, surveillent le système, alertent en cas de divergence, et ne lâchent jamais.

### **La vigilance rationnelle**

Attention : les Sentinelles ne sont pas des complotistes. Elles ne présument pas la fraude, elles vérifient. Si le système converge, elles le valident publiquement. S'il diverge, elles demandent des explications. C'est une vigilance rationnelle, non une paranoïa.

## **4. La philosophie de l'éducation à la lucidité**

### **Le problème de la confiance aveugle**

Le système actuel repose sur un principe simple : « Faites-nous confiance, nous sommes l'État, nous sommes honnêtes. » Pendant longtemps, ce principe a fonctionné, parce que la confiance institutionnelle était haute et que les citoyens croyaient en la probité de l'État.

### **L'effondrement de la confiance**

Cette confiance s'est aujourd'hui largement effondrée : 78 % des Français n'ont pas confiance dans la politique (Cevipof, 2026) ; l'abstention a atteint 28 % au second tour de la présidentielle de 2022 ; et 56 % des 18-24 ans ne sont pas allés voter au premier tour des municipales de 2026. La foi aveugle ne fonctionne plus.

Face à ce constat, l'État tente l'option A : « Faites-nous confiance, vraiment, on vous le promet. » Résultat : un échec, car les promesses ne suffisent plus

à elles seules. Le ShadowVote propose l'option B : « Ne nous faites pas confiance. Vérifiez. » Résultat espéré : la confiance n'est plus nécessaire, la preuve suffit.

C'est un changement de paradigme :

De...	À...
La foi	La lucidité
La croyance	La vérification
La passivité	La responsabilité

### **L'éducation à la lucidité**

La lucidité n'est pas le cynisme. Le cynique dit : « Tout est pourri, rien ne sert à rien, je n'y crois plus » — et le résultat est l'apathie, l'abstention, la capitulation. La Sentinelle dit : « Le système peut être opaque, je vais vérifier ; s'il est propre, je le validerai ; sinon, je le dénoncerai » — et le résultat est la vigilance active, l'audit permanent, le contrôle citoyen.

Le cynique	La Sentinelle
Abandonne	S'engage
Subit	Vérifie
Capitule	Contrôle

Le ShadowVote se veut ainsi l'antidote au cynisme.

### **Racines contre fruits, un rappel**

Revenons à la philosophie centrale de cet ouvrage, posée au Chapitre 3. Les fruits, ce sont les symptômes visibles du système : les taxes, les lois jugées injustes, les scandales, les mensonges politiques. Les racines, c'est la structure profonde du système : l'opacité, le monopole institutionnel, l'impossibilité de vérifier.

Les mouvements classiques attaquent les fruits — « Baissez les taxes ! », « Changez cette loi ! », « Démissionnez ! » Le système cède alors sur quelques fruits, mais les racines restent intactes, et les fruits pourris repoussent. Le ShadowVote, lui, attaque les racines — « Donnez-nous la preuve que nos votes comptent », « Laissez-nous vérifier », « Prouvez votre honnêteté. » Si les racines de l'opacité sont coupées, les fruits pourris — scandales, fraudes — ne peuvent plus pousser. C'est précisément parce qu'elle vise les racines plutôt que les fruits que cette lucidité individuelle a vocation à devenir une stratégie collective : c'est l'objet de la section suivante.

## **5. Le silence comme arme stratégique**

### **La révolution silencieuse**

La plupart des révolutions sont bruyantes : cris, slogans, violences, médias, arrestations. La Démocratie de l'Ombre, elle, est silencieuse. Pas de manifestation. Pas de blocage. Pas de violence. Pas de leaders médiatiques. Juste des millions de citoyens qui, tranquillement, votent deux fois.

### **Pourquoi le silence est-il puissant ?**

*Raison 1 : il désarme la répression.* L'État sait gérer les manifestations — CRS, gaz lacrymogène, arrestations. Il ne sait pas gérer des citoyens qui vérifient pacifiquement leur propre vote. Que ferait-il ? Interdire de vérifier ? Ce serait un aveu.

*Raison 2 : il préserve la sympathie publique.* Les mouvements violents perdent la sympathie des citoyens modérés — les Gilets Jaunes ont ainsi perdu une partie de leur capital de sympathie lorsque les images de vitrines brisées ont saturé les médias. Le ShadowVote, lui, ne casse rien : il vérifie. Il est, de ce fait, difficile à diaboliser.

*Raison 3 : il crée un effet de surprise.* Le système attend la confrontation classique — manifestations, grèves — et dispose de protocoles pour la gérer. Le ShadowVote arrive par une porte que personne ne garde. Quand l'État réalise qu'une part significative des électeurs utilise le ShadowVote, il est déjà trop tard : la preuve est là, publique, inaltérable.

### **Le pouvoir du nombre dans le silence**

Nombre de Sentinelles	Impact
1 Sentinelle	Invisible
10 000 Sentinelles	Anecdotique
100 000 Sentinelles	Intéressant
1 million de Sentinelles	Pression morale
5 millions de Sentinelles	Incontournable

À partir d'environ 10 % de participation, le ShadowVote devient un fait politique majeur : les médias en parlent, les responsables politiques doivent réagir, l'État ne peut plus l'ignorer. Et tout cela sans un seul slogan, sans une seule manifestation, sans une once de violence — juste la puissance tranquille de la vérification de masse.

## **6. Ce qui différencie le ShadowVote des autres mouvements**

### **Comparaison avec les mouvements classiques**

Mouvement	Objectif	Méthode	Résultat (analyse de l'auteur)
Gilets Jaunes	Changement fiscal + RIC	Manifestations, blocages	Échec (épuisement)
Nuit Debout	Refonder la	Occupations,	Échec

	démocratie	débats	(récupération politique)
Pétitions en ligne	Pression symbolique	Signatures en ligne	Le plus souvent sans suite
Mouvements politiques classiques	Prise de pouvoir	Élections	Échec, ou récupération par un parti
ShadowVote	Vérification permanente	Vote parallèle + blockchain	En cours

### **Ce qui rend le ShadowVote unique**

Il n'a pas de leader — donc il est difficile à décapiter. Il ne recourt pas à la violence — donc il est difficile à réprimer. Il n'est adossé à aucun parti — donc il est difficile à récupérer. Il ne porte aucune revendication négociable — sa seule demande est la preuve. Sa technologie est décentralisée — donc difficile à censurer.

### **Le ShadowVote n'est pas un parti politique**

La différence est fondamentale. Un parti veut prendre le pouvoir. Le ShadowVote veut surveiller le pouvoir. Un parti dit : « Votez pour nous, on va tout changer. » Le ShadowVote dit : « Votez pour qui vous voulez, mais vérifiez. »

### **Trans-partisan**

Le ShadowVote est trans-partisan. Les Sentinelles peuvent être de gauche, de droite, du centre, écologistes, ou abstentionnistes repenties — peu importe leur étiquette. Toutes et tous veulent la même chose : la preuve.

### **Conclusion du chapitre : une révolution sans violence**

La Démocratie de l'Ombre n'est pas une utopie. C'est une stratégie — une stratégie qui a fait ses preuves dans l'histoire, de Gandhi et le sel au Mur de Berlin, en passant par le boycott de Montgomery : le retrait du consentement à l'opacité.

Notre méthode tient en quatre refus et une affirmation. Nous ne demandons pas la permission. Nous ne mendions pas la réforme. Nous ne cassons rien. Nous construisons à côté. Et quand suffisamment de Sentinelles auront vérifié, le système officiel devra choisir : converger, et gagner en légitimité, ou diverger, et perdre toute crédibilité. Dans les deux cas, nous gagnons.

Les Sentinelles ne crient pas. Elles vérifient.

### **Transition vers le Chapitre 8**

Ce chapitre a posé un premier seuil : autour de 10 % de participation, le ShadowVote devient un fait politique incontournable. Le chapitre suivant

affine ce mécanisme et montre qu'un mouvement social peut basculer bien avant d'atteindre une telle masse — dès qu'une minorité déterminée, parfois de l'ordre de 1 % d'une population, atteint le point de bascule sociologique qui rend sa diffusion irréversible. Nous y verrons comment cette stratégie de diffusion virale transforme un mouvement silencieux en mouvement irrésistible.

La contagion commence.

# CHAPITRE 8

## LE BASCULEMENT DU 1 %

« Une minorité déterminée peut changer le monde. En fait, c'est la seule chose qui l'ait jamais fait. »

— citation largement diffusée sous le nom de Margaret Mead, dont l'origine exacte n'a jamais été retrouvée dans ses écrits

### Introduction : le point de non-retour

Dans le chapitre précédent, nous avons vu ce qu'est la Démocratie de l'Ombre : son architecture, ses garanties, son fonctionnement. Dans ce chapitre, nous allons voir comment elle pourrait se propager. Car un mouvement ne gagne pas par la force. S'il gagne, c'est par la contagion.

### La question centrale

Combien de Sentinelles faut-il pour que le ShadowVote devienne incontournable ?

La réponse tient en deux chiffres, pas un seul — et c'est la première chose à clarifier, car le titre même de ce chapitre repose sur elle.

**1 %**, c'est le seuil de visibilité sociale : le moment où le ShadowVote cesse d'être une curiosité de niche pour devenir un fait que la presse, les partis et les institutions commencent à commenter.

**10 %**, c'est le seuil de bascule structurelle : le moment où le mouvement devient réellement incontournable, au sens où aucune décision publique sur le sujet ne peut plus se prendre en l'ignorant.

« Le basculement du 1 % » désigne donc le déclenchement du processus — le point à partir duquel la dynamique de contagion s'enclenche et commence à s'auto-entretenir — et non son aboutissement, qui se situe plus loin. Entre les deux, il y a une phase de croissance qui se compte en mois, parfois en années, et dont rien ne garantit par avance ni la vitesse ni même l'issue. C'est cette mécanique, avec ses hypothèses et ses limites, que ce chapitre se propose de décrire.

### Ce que vous allez comprendre

- pourquoi le seuil de 1 % peut suffire à amorcer une dynamique de bascule (sociologie du point de bascule) ;
- ce qu'un exercice de scénario-planning sur un soir d'élection peut apprendre au ShadowVote, sans jamais le confondre avec une prédiction ;

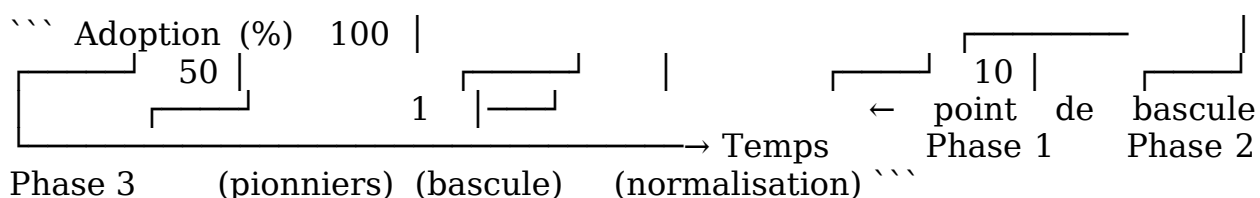
- comment une pression morale peut, dans certaines conditions, renverser la charge de la preuve ;
- pourquoi la contagion, une fois amorcée, est difficile à arrêter — et ce qui pourrait malgré tout la freiner.

## 1. La science du point de bascule

### Le concept de « tipping point »

En 2000, le journaliste Malcolm Gladwell publie *The Tipping Point* (« Le Point de bascule »), un ouvrage devenu culte dans la vulgarisation sociologique. Sa thèse centrale : les grandes transformations sociales ne nécessitent pas une majorité. Elles nécessitent une minorité active qui atteint un seuil critique ; passé ce seuil, la contagion peut devenir exponentielle.

Gladwell illustre cette idée par des exemples variés : une tendance vestimentaire qui décolle dès qu'une poignée d'influenceurs l'adopte ; une technologie dont l'usage s'accélère brutalement une fois qu'une frange significative de la population s'y est convertie ; un mouvement social qui bascule lorsque quelques milliers de prises de parole créent un effet d'entraînement disproportionné par rapport à leur nombre. Ce sont des illustrations, pas des lois : la vitesse et l'ampleur d'un basculement dépendent fortement du sujet, du contexte et du moment. Elles suffisent néanmoins à poser une intuition utile — un mouvement ne progresse pas de façon linéaire, mais par paliers, avec une phase de démarrage lente suivie d'une accélération brutale.



Phase	Part de la population	Dynamique
Phase 1 — les pionniers	0-1 %	Croissance lente, quasi invisible médiatiquement
Phase 2 — le basculement	1-10 %	Croissance rapide, entrée dans le débat public
Phase 3 — la normalisation	10-50 %	L'usage devient courant, mainstream

**Pourquoi le seuil de 1 % peut déclencher la dynamique : l'étude de Centola**

Au-delà de l'intuition de Gladwell, une étude expérimentale a cherché à mesurer ce phénomène plus rigoureusement. En 2018, le sociologue Damon Centola et son équipe (université de Pennsylvanie) publient dans la revue *Science* une expérience menée auprès de groupes en ligne, où une minorité de participants « engagés » tentait de faire adopter une nouvelle convention contre l'usage établi du groupe.

Résultat le plus souvent rapporté de cette étude : lorsque la minorité engagée avoisine un quart des membres du groupe — de l'ordre de 25 % —, la nouvelle convention finit presque toujours par s'imposer, et relativement vite. En deçà, le basculement devient plus incertain, plus lent, et parfois n'a pas lieu. Selon les conditions expérimentales et les répliques ultérieures de ce type de recherche, les seuils rapportés varient : les travaux antérieurs les situaient entre 10 % et 40 %, ce qui reste un ordre de grandeur, pas un chiffre unique et universel.

Part de « militants » engagés	Issue observée
25 % et plus (Centola et al., 2018)	La nouvelle convention s'impose rapidement
En dessous de 25 % (Centola et al., 2018)	Les tentatives de la minorité échouent
Études antérieures (modèles et expériences)	Seuils situés entre 10 % et 40 % selon les conditions
Modèle économique classique	Seuil supposé d'au moins 51 %

Source vérifiée : Centola, D., Becker, J., Brackbill, D., Baronchelli, A. (2018), « Experimental evidence for tipping points in social convention », *Science*, vol. 360, n° 6393, p. 1116-1119.

Il faut être honnête sur la portée de ce résultat. Centola mesure le basculement d'une norme sociale dans de petits groupes expérimentaux fermés, pas le résultat d'un scrutin national contesté par des millions de personnes. Le ShadowVote emprunte l'intuition du seuil critique — une minorité organisée peut faire bouger un ensemble bien plus grand qu'elle — sans prétendre que le chiffre exact de l'étude se transpose tel quel à l'échelle d'un pays. C'est une source d'inspiration scientifique sérieuse, pas une preuve directe transposable.

### **Application au ShadowVote : deux seuils, pas un**

La France compte environ 50 millions d'électeurs inscrits sur les listes électorales (50,2 millions en février 2026, selon l'Insee).

Pourcentage	Nombre de Sentinelles	Ce que cela signifierait
1 %	500 000	Seuil de visibilité : un fait social repérable et commenté, mais

		encore marginal politiquement
5 %	2,5 millions	Seuil de pression : le sujet s'installe dans le débat public
10 %	5 millions	Seuil de bascule structurelle : le ShadowVote devient incontournable dans la fabrication de la décision publique

Ces seuils constituent une hypothèse de travail, construite par analogie avec la littérature sur la diffusion sociale — ils ne prétendent pas reproduire mécaniquement le chiffre mesuré par Centola, dont l'expérience portait sur un objet différent (un groupe fermé d'une vingtaine de personnes, non une population nationale). Concrètement, l'idée défendue ici est la suivante : à partir de 500 000 utilisateurs, il deviendrait difficile de présenter le ShadowVote comme un simple gadget militant ; à partir de 5 millions, il deviendrait difficile de l'écarter du débat démocratique.

### Les trois vagues d'adoptants

En reprenant un schéma classique de la diffusion de l'innovation — popularisé notamment par le sociologue Everett Rogers —, on peut décrire trois vagues successives d'adoptants.

*Vague 1 — les innovateurs (0 à 2,5 %).* Développeurs, militants de la transparence, citoyens déçus du fonctionnement institutionnel. Julien, 31 ans, développeur (chapitre 1), ou Marie, 38 ans, développeuse blockchain (chapitre 7), illustrent ce profil. Ils adoptent l'outil dès son lancement, contribuent au code ouvert, hébergent des nœuds, en parlent autour d'eux. Leur rôle : construire l'infrastructure et amorcer le bouche-à-oreille. Nombre nécessaire, dans cette hypothèse : entre 500 000 et 1,25 million.

*Vague 2 — les adoptants précoces (2,5 à 15 %).* Citoyens engagés, enseignants, journalistes, étudiants politisés — Sophie, 42 ans, professeure (chapitre 6), ou Inès, 24 ans, étudiante (chapitre 1), si elle se laisse convaincre. Ils utilisent le ShadowVote après en avoir entendu parler, en parlent à leur entourage, relaient sur les réseaux. Leur rôle : créer la masse critique qui attire l'attention médiatique. Nombre nécessaire : entre 1,25 et 7,5 millions.

*Vague 3 — la majorité pragmatique (15 à 60 %).* Les citoyens qui veulent avant tout que l'outil fonctionne simplement — Jean, 68 ans, retraité (chapitre 6), ou Odette, 82 ans, aidée par sa petite-fille. Ils adoptent le ShadowVote parce que c'est devenu un geste courant, sans militer

activement. Leur rôle : normaliser l'usage. Nombre nécessaire : entre 7,5 et 30 millions.

Le point clé : il ne s'agirait pas de convaincre d'emblée 50 millions d'électeurs, mais environ 500 000 innovateurs. Si la dynamique décrite plus haut se vérifie, le reste pourrait suivre — mais rien ne le garantit mécaniquement : c'est une hypothèse de diffusion, pas une certitude.

---

## **2. Les trois scénarios de basculement : un exercice de scénario-planning**

Avant d'aller plus loin, une précision s'impose. Ce qui suit n'est pas une prédiction. C'est un exercice de scénario-planning — une méthode courante en stratégie et en gestion des risques, qui consiste à décrire plusieurs futurs possibles pour s'y préparer, sans prétendre savoir lequel se réalisera. Les chiffres qui suivent sont illustratifs : ils servent à raisonner sur des ordres de grandeur, pas à annoncer un résultat.

Imaginons que le ShadowVote ait atteint, un soir de scrutin, un taux de participation significatif — de l'ordre de 10 % des électeurs. Trois familles de scénarios se dessinent alors.

### **Scénario A : convergence**

Si l'on projette une situation où les résultats du ShadowVote et ceux de l'urne officielle se rejoignent à quelques dixièmes de point près, l'État pourrait s'en prévaloir : le système fonctionne, la confiance est restaurée. Les Sentinelles pourraient, de leur côté, revendiquer une validation citoyenne des résultats. Dans cette hypothèse, aucune des deux parties n'aurait intérêt à contester l'autre. Un tel scénario, s'il se répétait à plusieurs scrutins, pourrait progressivement banaliser l'usage du ShadowVote — jusqu'à, éventuellement, une forme de reconnaissance institutionnelle. Ce serait un horizon possible, pas un aboutissement acquis.

### **Scénario B : écart minime**

Un autre scénario possible verrait apparaître un écart faible mais non négligeable, de l'ordre de 1 à 3 points. Plusieurs explications seraient alors envisageables, sans qu'on puisse trancher entre elles sans vérification : un biais d'échantillon, la population utilisatrice du ShadowVote étant probablement plus jeune, plus urbaine et plus connectée que la moyenne des électeurs ; des erreurs mineures de dépouillement du côté de l'urne officielle (cf. chapitre 2) ; ou, dans l'hypothèse la plus sensible, des indices de dysfonctionnement localisé dans quelques bureaux.

Face à un tel écart, l'État aurait le choix entre ordonner un recomptage ciblé — ce qui permettrait de trancher empiriquement — ou l'attribuer à

une marge d'erreur statistique, au risque d'alimenter une demande de transparence plus insistante. Dans cette seconde hypothèse, le ShadowVote pourrait, avec le temps, s'installer comme un garde-fou officieux : sans reconnaissance officielle, mais avec une influence réelle sur les pratiques de dépouillement.

### **Scénario C : divergence marquée**

Le scénario le plus disruptif serait celui d'un écart de plusieurs points sur un ou plusieurs candidats — un ordre de grandeur qui, s'il se confirmait, ne pourrait plus raisonnablement être attribué au seul bruit statistique. On peut imaginer, dans cette hypothèse, une couverture médiatique importante, des réactions politiques contrastées — le candidat avantagé par l'écart réclamant un recomptage, celui qui en pâtirait rappelant l'absence de valeur légale du ShadowVote —, et une pression croissante pour une vérification indépendante.

L'État aurait alors, schématiquement, trois postures possibles : recompter et, le cas échéant, reconnaître une erreur — l'option la plus coûteuse politiquement à court terme, mais aussi celle qui restaurerait le plus de confiance ; recompter et confirmer l'urne officielle, ce qui imposerait d'expliquer l'écart observé par des éléments vérifiables (biais démographique, défaillance ou manipulation du dispositif citoyen) ; ou refuser tout recomptage au nom de l'absence de valeur légale du ShadowVote, ce qui, dans cette hypothèse, risquerait d'aggraver la défiance plutôt que de la clore.

Ce triptyque ne prétend pas épuiser toutes les possibilités, et aucun des trois scénarios n'est plus « probable » que les autres au vu des éléments disponibles aujourd'hui. Il montre en revanche qu'un dispositif de vérification citoyenne change la nature du débat en cas de doute : au lieu d'une contestation sans preuve, il introduirait un élément de comparaison chiffré, qui devrait être discuté sur le fond plutôt qu'écarté par principe.

---

## **3. La pression morale : un renversement possible de la charge de la preuve**

Aujourd'hui, contester une élection revient, pour l'essentiel, à devoir apporter la preuve d'une fraude — une charge lourde, qui décourage la plupart des contestations, fondées ou non.

Avec un dispositif de vérification citoyenne suffisamment répandu, cette dynamique pourrait s'inverser : en cas d'écart significatif et documenté entre l'urne officielle et le décompte parallèle, ce serait à l'autorité qui gère le scrutin d'expliquer cet écart de façon convaincante — non plus au citoyen isolé de prouver l'anomalie. Ce renversement n'a rien d'automatique ni de garanti : il suppose que le ShadowVote ait atteint une taille et une

crédibilité suffisantes pour que son écart ne puisse pas être balayé d'un revers de main. Mais c'est, potentiellement, l'apport le plus original du dispositif : transformer une défiance diffuse, difficile à objectiver, en un écart chiffré que les institutions doivent au moins commenter.

### **L'effet de légitimité**

Des travaux classiques de psychologie sociale — les expériences de Stanley Milgram sur l'obéissance à l'autorité (1963) et celles de Solomon Asch sur le conformisme au jugement du groupe (1951) — suggèrent que l'obéissance à une autorité dépend largement de sa légitimité perçue : elle se maintient tant que cette légitimité n'est pas sérieusement mise en doute, et peut s'éroder rapidement dès qu'elle l'est.

Appliqué à un scrutin : un scénario de convergence entre urne et ShadowVote renforcerait la légitimité perçue de l'institution ; un scénario de divergence documentée l'affaiblirait — parfois indépendamment même de ce que révélerait une enquête ultérieure. Le simple fait qu'un doute chiffré existe peut suffire à modifier la perception publique, ce qui rend d'autant plus important, pour toutes les parties, qu'un écart, s'il apparaît, soit expliqué plutôt qu'ignoré.

### **Un outil difficile à disqualifier sur le fond, pas impossible à combattre**

L'État pourrait chercher à décrédibiliser le ShadowVote en le présentant comme un outil de déstabilisation. L'argument se heurterait à des caractéristiques vérifiables du dispositif : un code ouvert et auditable par quiconque, une architecture décentralisée sans serveur central unique, des votes consultables, un mécanisme de vérification mathématique. Plus une méthode est publique et vérifiable, plus sa disqualification par simple déclaration devient difficile. Cela ne la rend pas impossible pour autant : une campagne de communication peut affecter l'opinion à court terme, avant même qu'une vérification indépendante ait eu le temps de circuler aussi largement que l'accusation initiale. La transparence du dispositif atténue ce risque réputationnel ; elle ne l'annule pas.

---

## **4. La contagion : comment un mouvement se propage**

### **Trois vecteurs de propagation**

*Le bouche-à-oreille.* Chaque Sentinelle active convainc, en moyenne, quelques personnes de son entourage. Si cet effet se maintient sur plusieurs vagues de recrutement successives, il pourrait suffire, en quelques mois à quelques années, à faire passer un mouvement de quelques milliers à plusieurs centaines de milliers d'utilisateurs — le rythme exact dépendant

fortement du contexte politique et médiatique du moment, et ne pouvant pas être prédit avec précision à l'avance.

*Les réseaux sociaux.* Un contenu bien conçu — vidéo explicative courte, témoignage, comparaison visuelle entre une urne opaque et un registre vérifiable — peut toucher, en quelques jours, une audience très supérieure au nombre de personnes réellement convaincues. La plupart des personnes touchées ne s'engageront pas ; mais une conversion, même minoritaire, peut représenter, à grande échelle, plusieurs dizaines de milliers de nouveaux utilisateurs par contenu viral.

*Les médias traditionnels.* Un mouvement qui franchit un seuil de visibilité suffisant finit, en pratique, par intéresser d'abord les médias spécialisés, puis les médias généralistes, puis, éventuellement, la télévision et la presse internationale. Chaque étape élargit fortement l'audience potentielle — sans qu'aucun calendrier précis puisse être garanti à l'avance.

Phase	Horizon indicatif	Dynamique	Type de couverture
Démarrage	premiers mois	Croissance organique, lente	Médias spécialisés
Accélération	1 à 2 ans	Croissance rapide	Médias généralistes
Massification	2 à 3 ans	Croissance de masse	Télévision, presse quotidienne
Normalisation	au-delà	Stabilisation	Éventuelle reconnaissance institutionnelle

Ces durées sont des ordres de grandeur hypothétiques, pas un calendrier engagé.

### **Des précédents historiques, à lire avec leurs vraies échelles de temps**

*#MeToo (2017).* L'affaire Weinstein éclate en octobre 2017. Une dizaine de jours plus tard, l'actrice Alyssa Milano relance le mot-clic *#MeToo* sur les réseaux sociaux — une expression forgée dès 2006 par la militante Tarana Burke. Selon les chiffres communiqués à l'époque par les plateformes, plusieurs millions de publications et réactions mentionnant *#MeToo* sont recensées dès les premières 24 à 48 heures. Le mouvement se poursuit et s'amplifie durant les mois suivants, jusqu'à devenir un phénomène mondial et à peser sur des évolutions législatives dans plusieurs pays. Facteur clé : chaque témoignage rendait le suivant plus légitime à formuler.

*Les Gilets Jaunes (2018).* Le mouvement naît d'un appel relayé sur les réseaux sociaux à l'automne 2018. Dès le jour de la première mobilisation, le 17 novembre 2018, le ministère de l'Intérieur dénombre près de 283 000

manifestants sur l'ensemble du territoire. Le mouvement se maintient ensuite sur plusieurs mois, avec des pics et des reflux, jusqu'à devenir un sujet durable du débat public. Facteur clé : l'effet de réseau, amplifié par une forte couverture médiatique.

*Le vote blanc (2010-2017).* La comptabilisation distincte du vote blanc, longtemps réclamée par certains observateurs, reste marginale jusqu'à son inscription dans la loi en 2014, qui reconnaît le vote blanc sans toutefois l'assimiler aux suffrages exprimés. Au second tour de la présidentielle de 2017, les bulletins blancs représentent 8,5 % des votants, un niveau record. Facteur clé : la légitimation progressive, par la loi, d'un geste citoyen jusque-là marginal.

Ces trois exemples partagent des ingrédients qu'on retrouve, par hypothèse, dans le pari du ShadowVote : une légitimité morale perçue par ceux qui y participent, une facilité d'adoption, une viralité qui tient à ce que chaque utilisateur peut devenir un relais, et une couverture médiatique qui devient probable dès qu'un écart ou une controverse apparaît. Il faut cependant noter que ces trois exemples sont des succès : ils ne disent rien des mouvements comparables qui n'ont jamais dépassé leur phase de démarrage — et de tels échecs existent aussi, même s'ils sont, par nature, moins documentés et moins médiatisés.

---

## **5. Pourquoi l'État aurait du mal à l'arrêter — et où se situent les vraies limites**

Un mouvement qui grandit attire aussi la résistance. Voyons les principaux leviers dont disposerait un État pour freiner un dispositif comme le ShadowVote, et pourquoi chacun d'eux est plus compliqué à actionner qu'il n'y paraît — sans que cela signifie qu'aucun ne présente de risque réel.

### **Interdire le dispositif**

Le ShadowVote se présente comme un vote citoyen parallèle, sans valeur légale — un comptage indépendant proche, dans son principe, du *Parallel Vote Tabulation* (PVT) que pratiquent depuis des décennies des organisations d'observation électorale internationale comme le Carter Center ou le National Democratic Institute. Il ne remplace pas le vote officiel : il le compare.

C'est précisément ce qui le distingue, sur le plan juridique, d'une fraude ou d'une atteinte au processus électoral encadré par le code électoral. Un dispositif de ce type devrait néanmoins composer, en France, avec un cadre juridique réel et non négligeable : le Règlement général sur la protection des données (RGPD) et le contrôle de la CNIL, qui encadrent strictement la collecte et le traitement de données susceptibles de révéler une opinion politique — un vote individualisé, même chiffré et pseudonymisé, peut y être

soumis ; et le code électoral lui-même, qui pourrait être mobilisé si le dispositif entretenait une ambiguïté avec le scrutin officiel, par exemple dans sa présentation publique ou dans sa proximité avec les opérations de vote.

C'est pourquoi la conception du ShadowVote, décrite au chapitre 7, insiste sur son caractère strictement parallèle et non officiel : un outil de vérification citoyenne pensé, autant que possible, pour respecter les exigences du RGPD — minimisation des données, consentement, anonymisation — plutôt que pour les contourner. Cette conception ne garantit pas l'absence de contentieux : la CNIL pourrait exiger des ajustements, voire suspendre temporairement un traitement de données jugé non conforme, et une procédure judiciaire, même perdue au fond par l'État, peut ralentir ou fragiliser un mouvement pendant sa phase la plus critique. Une interdiction pure et simple de l'outil se heurterait, elle, à la liberté d'expression protégée par l'article 10 de la Convention européenne des droits de l'homme, et produirait vraisemblablement un effet Streisand — la contestation de l'outil amplifiant sa visibilité plutôt que de l'éteindre.

### **Attaquer l'infrastructure technique**

Un dispositif décentralisé, reposant sur de nombreux nœuds hébergés dans plusieurs pays et sur un code ouvert dupliqué de multiples fois, est structurellement difficile à faire disparaître par une action technique unique : il n'y a pas de serveur central dont la neutralisation suffirait. Cela ne rend pas pour autant toute perturbation impossible. Un blocage temporaire de noms de domaine, une pression sur des hébergeurs nationaux ou sur les plateformes de distribution d'applications mobiles peut ralentir l'accès pour une partie des utilisateurs, le temps que des alternatives — miroirs, VPN, autres canaux de diffusion — prennent le relais. C'est une gêne possible, pas nécessairement une extinction.

### **Chercher à discréditer le mouvement**

Une stratégie classique consisterait à présenter le dispositif comme téléguidé par un acteur hostile. L'argument se heurterait au caractère public du code, des comptes, et — si le financement est organisé sur la blockchain — de sa traçabilité : autant d'éléments vérifiables par quiconque prend le temps de les examiner. Cela ne rend pas pour autant une telle campagne inefficace à court terme : la désinformation peut affecter l'opinion publique avant même qu'une vérification indépendante ait eu le temps de circuler aussi largement que l'accusation initiale. C'est un risque réputationnel réel, que la transparence du dispositif atténue sans l'annuler complètement.

### **Récupérer politiquement le mouvement**

Un parti qui afficherait un soutien exclusif au ShadowVote s'exposerait à une réponse simple de la part des Sentinelles : le dispositif se veut trans-

partisan, il vérifie tous les votes, y compris ceux du parti qui prétendrait se l'approprier. Cette réponse protège la légitimité du mouvement — à condition que ses porte-parole successifs continuent effectivement à refuser toute étiquette partisane, ce qui n'a rien d'acquis dans la durée.

---

## **Conclusion du chapitre : une dynamique plausible, pas une garantie**

Le basculement du 1 % n'est pas une promesse. C'est une hypothèse construite à partir de recherches sérieuses sur la diffusion sociale — l'intuition de Gladwell, l'expérience de Centola — et transposée, avec les précautions qui s'imposent, à un projet politique d'un genre différent.

Les seuils retenus dans ce chapitre restent une grille de lecture, pas des paliers garantis : à 500 000 utilisateurs, le ShadowVote deviendrait un fait social visible ; à 5 millions, il deviendrait difficile à ignorer dans le débat public. Entre les deux, trois familles de scénarios sont envisageables un soir de scrutin — convergence, écart minime, divergence marquée — et dans chacune d'elles, un dispositif de vérification citoyenne changerait la nature du débat, en donnant un point de comparaison chiffré à une défiance qui, aujourd'hui, reste largement sans preuve.

Si la contagion se produit, elle ne tiendra ni à la force ni à la contrainte, mais à l'accumulation d'éléments vérifiables que chacun peut examiner par lui-même. Un système peut ignorer mille utilisateurs. Il peut se permettre de ne pas commenter cent mille signalements. Il lui deviendrait nettement plus difficile de ne rien dire face à plusieurs millions de vérifications indépendantes et documentées.

---

## **Transition vers le chapitre 9**

Ce chapitre a posé les grandes lignes d'une dynamique de diffusion possible, avec ses hypothèses et ses limites. Reste la question la plus concrète : comment, très précisément, un tel mouvement se lancerait-il ? Le chapitre suivant propose une feuille de route — les phases de déploiement, les premières actions, les conditions pratiques d'un lancement. La théorie s'arrête ici. La mise en œuvre commence.

# CHAPITRE 9

## LA FEUILLE DE ROUTE CITOYENNE

« *Un plan sans action n'est qu'un rêve. Une action sans plan n'est qu'un chaos.* » — dicton populaire, souvent présenté comme un proverbe japonais sans source primaire confirmée

### Introduction : de la vision au plan d'action

Nous avons le diagnostic (Partie I). Nous avons la solution technique (Partie II). Nous avons la philosophie et la stratégie (chapitres 7 et 8).

Maintenant, il faut un plan.

Un plan concret, daté, budgété, avec des étapes claires et des responsabilités définies. Ce chapitre est le cahier des charges de la révolution.

### Ce que vous allez savoir

À la fin de ce chapitre, vous saurez :

- Les 4 phases de déploiement, de 0 à 36 mois et plus
- Ce qu'il faut faire MAINTENANT (Phase 1)
- Comment gérer les risques : attaques, censure, échec
- Le Plan B si le ShadowVote échoue

Parce qu'un manifeste sans plan d'action n'est qu'un rêve. Et nous ne rêvons pas. Nous agissons.

---

### Pourquoi pas 2027 ? Deux horizons, un seul plan

Posons tout de suite la question que vous êtes en train de vous poser.

Ce livre sort en 2026. L'élection présidentielle aura lieu les 18 avril et 2 mai 2027 (dates annoncées par le gouvernement en juillet 2026) — quelques mois plus tard seulement. Les chapitres 5 et 6 vous ont montré un citoyen votant grâce à un ShadowVote pleinement opérationnel ce jour-là. Or le calendrier détaillé dans les pages qui suivent est sans détour : le prototype n'est audité et achevé qu'au mois 18, le premier test en conditions réelles ne se termine qu'au mois 30, et une extension nationale légale n'est même envisageable qu'après le vote d'une loi puis deux années d'évaluation obligatoire. Vous êtes en droit de vous demander comment ces deux récits tiennent ensemble.

Réponse honnête : ils ne racontent pas la même chose. Il faut distinguer deux horizons, et nous les assumons tous les deux, dès maintenant, noir sur blanc.

**L'horizon politique : 2027.** Quel que soit le mois exact de la sortie de ce livre en 2026, l'élection présidentielle d'avril 2027 tombera au mieux en toute fin de Phase 1, au pire en tout début de Phase 2 — c'est-à-dire à un moment où le mouvement n'a, techniquement, rien de plus à montrer qu'un manifeste, une pétition et un collectif naissant. Aucun prototype, aucun test, aucune ville pilote ne seront prêts à cette date, et ce livre ne prétend pas le contraire. Ce que visent la sortie du livre, la pétition et ses 100 000 signatures, les groupes locaux et le collectif de Sentinelles, c'est l'échéance d'avril 2027 comme un jalon de pression et de visibilité — pas comme une date de mise en service, même partielle. Le but n'est pas que le ShadowVote remplace ou double l'urne officielle lors de cette élection précise. Le but est qu'au moment où les Français votent, le mouvement soit assez massif, assez crédible et assez documenté pour que la question de la vérifiabilité du vote s'impose dans le débat public, quels que soient les candidats en lice. C'est l'argument développé au chapitre 8 : il ne faut pas attendre d'avoir convaincu l'État avant l'élection, il faut construire d'ici là un rapport de force citoyen qui pèsera après.

**L'horizon technique et légal : le cycle électoral suivant.** Un outil de vote parallèle ne se construit pas, ne s'audite pas, ne se teste pas à grande échelle et ne se légalise pas en quinze mois. Le calendrier qui suit est sans ambiguïté : le prototype audité n'existe qu'à partir du mois 18, le premier test grandeur nature se conclut au mois 30, et la loi qui pourrait autoriser une extension nationale n'est déposée qu'à ce moment-là — avec, une fois votée, deux années d'évaluation obligatoire avant toute extension aux élections nationales (voir Article 4, section 5). Le déploiement national complet et légal vise donc, réalistement, l'échéance électorale de 2032 — municipales et présidentielle confondues — et non la présidentielle de 2027.

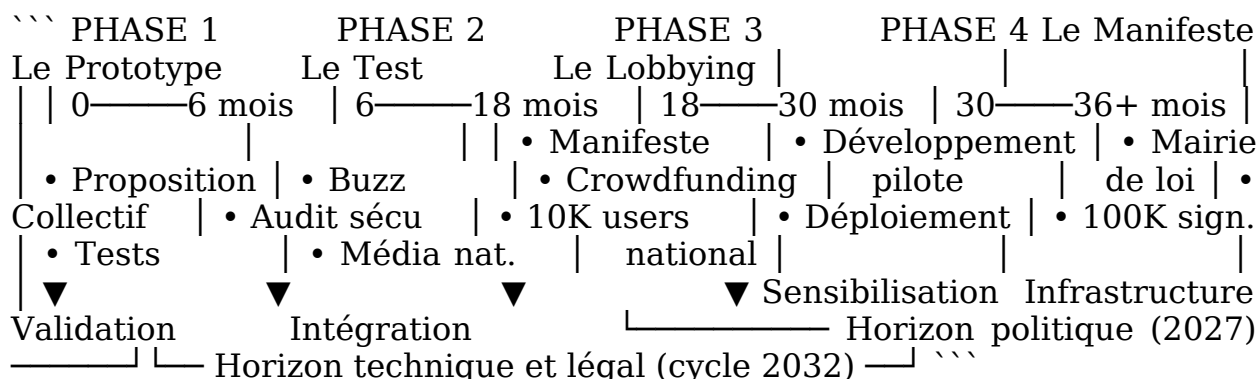
Ce n'est pas un aveu d'échec. C'est la reconnaissance honnête d'un fait simple : changer les règles du jeu démocratique prend du temps. Un système de vote parallèle bâclé pour tenir un délai politique serait exactement l'inverse de ce que ce livre défend : la preuve, pas la précipitation. Nous préférons un ShadowVote qui arrive plusieurs années plus tard et qui tient ses promesses de vérifiabilité, à un ShadowVote livré à temps pour 2027 et truffé de failles.

Retenez donc ceci pour lire tout ce chapitre. Chaque action des Phases 1 et 2 nourrit l'horizon politique de 2027 : mobilisation, preuve de concept, rapport de force. Chaque action des Phases 3 et 4 construit l'horizon technique et légal du cycle suivant : outil fiable, audité, encadré par la loi. Les deux horizons sont nécessaires. Aucun des deux ne remplace l'autre. Et

non, le ShadowVote ne sera pas prêt à remplacer l'urne en 2027 — nous l'écrivons ici, clairement, plutôt que de le laisser deviner.

## 1. Vue d'ensemble : les quatre phases

### Timeline globale (3 ans et plus)



Selon le mois exact de sortie du livre en 2026, l'élection d'avril 2027 tombe entre le mois 4 et le mois 8 environ après publication — c'est-à-dire à l'intérieur de la Phase 1 (le Manifeste) ou tout au début de la Phase 2 (le Prototype). Dans tous les cas de figure, bien avant qu'un prototype existe, qu'il soit audité ou qu'il ait quitté le stade de la conception. C'est précisément pour cela que 2027 est un jalon de pression, pas de déploiement : à cette date, le mouvement se compte en signatures et en Sentinelles, pas encore en lignes de code auditées.

### Objectifs par phase

Phase	Durée	Horizon	Objectif principal	Métrique de succès
Phase 1 — Le Manifeste	0-6 mois	Politique	Créer le mouvement	100 000 signatures à la pétition
Phase 2 — Le Prototype	6-18 mois	Politique	Construire l'outil	Prototype fonctionnel audité
Phase 3 — Le Test Pilote	18-30 mois	Technique et légal	Prouver la viabilité, localement	10 000 utilisateurs, test réussi
Phase 4 — Le Lobbying	30-36+ mois	Technique et légal	Encadrer légalement un déploiement futur	Loi votée ou adoption citoyenne de facto

---

## 2. PHASE 1 : Le Manifeste (0-6 mois)

Nous y sommes. C'est MAINTENANT.

**Objectif :** Créer le buzz. Lancer la pétition. Former le collectif citoyen.

**Livrable final :** 100 000 signatures et 1 000 Sentinelles actives.

### Mois 1-2 : Publication et lancement

#### Action 1 — Publication du manifeste

Support : livre papier (Amazon KDP, auto-édition), eBook payant (plateformes numériques), réseaux sociaux (diffusion virale).

Stratégie de lancement : publication du livre physique fin 2026, eBook payant simultané à un prix accessible pour maximiser la diffusion, campagne réseaux sociaux intensive.

#### Action 2 — Lancement de la pétition

Plateforme : Change.org (ou MesOpinions.com).

Titre de la pétition : « *Pour un vote vérifiable : nous exigeons le droit de prouver que notre voix compte* ».

Texte (300 mots maximum) :

En 2026, nous pouvons tracer un colis à 12 000 km, mais pas notre bulletin de vote.

28 % d'abstention. 78 % de défiance. Une génération entière qui décroche.

Nous ne demandons pas de réformer le système. Nous proposons de construire notre propre système de vérification.

Le ShadowVote : un vote citoyen parallèle, enregistré sur une blockchain publique et inaltérable, qui permet à chaque électeur de vérifier que sa voix a été comptée.

Nous demandons :

- Le droit d'expérimenter publiquement le ShadowVote en marge des scrutins, dès maintenant, dans une ville volontaire ;
- Un débat parlementaire sur l'intégration de la blockchain au processus électoral ;

- Un calendrier légal clair vers une intégration nationale — même si cela dépasse l'élection présidentielle de 2027.

Signez si vous pensez que vérifier son vote est un droit, pas un privilège.

Objectif : 100 000 signatures en 6 mois.

### **Action 3 — Campagne médiatique**

Cibles, par cercles concentriques :

- Médias de niche (mois 1) : sites d'information indépendants et spécialisés (par exemple Mediapart ou Reporterre), sites consacrés aux technologies (par exemple Korben ou Next), podcasts consacrés à la démocratie et au numérique.
- Médias mainstream (mois 2-3), cibles visées sans qu'aucun contact ait été pris à ce jour : Le Monde (rubrique Idées), Libération (chronique), France Inter (émission politique), C à Vous (débat TV).
- Médias internationaux (mois 4-6) : The Guardian (si buzz en France), BBC, New York Times (Op-Ed).

Stratégie de pitch, trois angles selon la cible :

- Angle 1 (progressistes) : « Comment la blockchain peut sauver la démocratie de l'abstention. »
- Angle 2 (tech) : « L'application qui permet à chacun de vérifier son vote. »
- Angle 3 (grand public) : « Fini de voter dans le noir : le mouvement qui exige la preuve. »

### **Action 4 — Réseaux sociaux**

- X (ex-Twitter) : compte @ShadowVote\_FR, hashtags #ShadowVote #NeCroisPlusVérifie #PlusJamaisSansPreuve, 5 tweets/jour (chiffres chocs, infographies, témoignages). Objectif : 10 000 followers en 6 mois.
- Instagram : compte @shadowvote.fr, visuels percutants (comparaison urne/blockchain), stories de témoignages de Sentinelles. Objectif : 5 000 followers.
- TikTok : vidéos courtes (30-60 secondes), format éducatif ou humoristique. Objectif : une vidéo virale (100K+ vues).
- YouTube : chaîne ShadowVote, vidéos explicatives (5-10 minutes), interviews d'experts (cryptographes, politologues). Objectif : 50 000 vues cumulées.

## **Mois 3-4 : Formation du collectif**

### **Action 5 — Création de la structure légale**

Avant toute collecte d'argent, il faut une structure légale.

Type	Avantages	Inconvénients
Association loi 1901	Facile à créer ; peut recevoir des dons ; transparente	Limitée en activité économique
Fondation reconnue d'utilité publique	Crédibilité maximum ; défiscalisation	18-24 mois de création ; contrôle étatique strict
SCIC	Gouvernance démocratique ; multi-parties prenantes	Complexe à créer

Recommandation : association loi 1901 en Phase 1.

- Nom : Association ShadowVote.
- Objet : promouvoir la transparence électorale via la technologie blockchain.
- Bureau minimum : président(e), trésorier(e), secrétaire général(e).
- Membres fondateurs : 7 à 10 personnes.
- Statuts publiés en ligne (transparence totale).

## **Action 6 — Formation des groupes locaux**

Objectif : 50 groupes locaux, dans des villes de plus de 50 000 habitants.

Outils : Discord (serveur national avec salons par ville), Telegram (groupes locaux), Meetup (événements physiques).

Activités : réunions mensuelles (café citoyen), ateliers d'initiation à la blockchain, stands sur les marchés et dans les gares (pétition papier), projections-débats.

## **Mois 5-6 : Préparation de la Phase 2**

### **Action 7 — Identification des partenaires**

- Partenaires techniques : laboratoires blockchain universitaires (Paris-Saclay, INRIA), entreprises tech (conseillers bénévoles), développeurs open-source (appel à contributions).
- Partenaires institutionnels : ONG de transparence (Transparency International France), think tanks démocratie (Terra Nova, Fondation Jean Jaurès), élus visionnaires de tous bords intéressés par le sujet.
- Partenaires médias : journalistes spécialisés (tech, politique), influenceurs citoyens engagés.

### **Action 8 — Cahier des charges technique**

Livrable : un document de 50 pages couvrant les spécifications fonctionnelles, les spécifications techniques (choix de blockchain, outils),

l'architecture système, le plan de sécurité (audits, tests d'intrusion) et le budget détaillé (développement et infrastructure). Ce document servira à la levée de fonds, au recrutement des développeurs et aux audits de sécurité.

## Budget Phase 1

Poste	Montant
Création de la structure légale	1 000 €
Communication (design, vidéos)	5 000 €
Événements (50 meetups × 100 €)	5 000 €
Juridique (consultations avocat)	3 000 €
Divers (imprévus)	4 000 €
<b>TOTAL PHASE 1</b>	<b>18 000 €</b>

Financement : contributions des fondateurs (8 000 €) et crowdfunding Ulule/KissKissBankBank (10 000 €, soit 100 personnes à 100 € chacune).

## Métriques de succès Phase 1

- 100 000 signatures à la pétition
- 1 000 Sentinelles actives (inscrites sur Discord/Telegram)
- 50 groupes locaux formés
- 10 articles dans des médias nationaux
- Association créée et déclarée
- Cahier des charges technique validé

Si ces six objectifs sont atteints, passage en Phase 2.

## 3. PHASE 2 : Le Prototype (6-18 mois)

**Objectif** : construire l'outil.

**Livrable final** : une application mobile et web fonctionnelle, auditée, testée avec 1 000 utilisateurs.

Rappel : cette phase se termine au mois 18, soit à peu près mi-2027. C'est elle qui absorbe le mois de l'élection présidentielle — l'outil y est en développement puis en tests internes, jamais en usage public.

### Mois 6-9 : Levée de fonds

#### Action 9 — Campagne de crowdfunding

Plateforme : Kickstarter ou Ulule. Objectif : 450 000 €.

Don	Contrepartie	Nombre attendu	Total
10 €	Remerciement	10 000 × 10 €	100 000 €

	nominatif		
50 €	Badge « Sentinelle fondatrice »	3 000 × 50 €	150 000 €
100 €	Badge + nom dans l'app	1 500 × 100 €	150 000 €
500 €	Tout + invitation au lancement	100 × 500 €	50 000 €
<b>Total</b>		<b>14 600 contributeurs</b>	<b>450 000 €</b>

Communication de campagne : vidéo Kickstarter professionnelle (3 minutes), relais médias, mobilisation des 1 000 Sentinelles actives (chacune visant à convaincre 15 donateurs).

### Action 10 — Compléments de financement

Si le crowdfunding est insuffisant :

- Subventions publiques : Union européenne (Horizon Europe, fonds innovation démocratique), régions (innovation sociale).
- Fondations privées : Open Society Foundations (démocratie), Ford Foundation, Omidyar Network (tech civique).
- Mécènes tech : entrepreneurs sensibles à la cause, approchés individuellement.

## Mois 9-15 : Développement

### Action 11 — Recrutement de l'équipe

Équipe cœur, 5 personnes salariées :

Poste	Profil	Salaire annuel
CTO (lead dev)	Développeur blockchain senior	70 000 €
Développeur full-stack	React Native + Node.js	50 000 €
Développeur blockchain	Solidity + Polygon	60 000 €
Designer UX/UI	Applications mobiles	45 000 €
Chef de projet	Gestion et communication	45 000 €
<b>Total masse salariale</b>		<b>270 000 €/an</b>

Contributeurs bénévoles (open-source) : 10 à 20 développeurs externes pour des contributions ponctuelles, et 5 à 10 testeurs QA bénévoles.

## **Action 12 — Développement agile**

Méthode : sprints de deux semaines.

- Mois 9-10, infrastructure : mise en place des serveurs (nœuds Polygon), architecture backend (API), base de données.
- Mois 11-12, smart contracts : contrat de vote en Solidity, tests unitaires, déploiement sur le testnet Polygon.
- Mois 13-14, application mobile : interface iOS/Android en React Native, intégration blockchain, mode senior (accessibilité).
- Mois 15, finitions : corrections de bugs, optimisations de performance, documentation utilisateur.

## **Action 13 — Audits de sécurité**

- Audit n° 1, code des smart contracts : cabinet externe (Trail of Bits, OpenZeppelin ou Kudelski Security), coût 50 000 €, durée 4 semaines, livrable : rapport public d'audit avec corrections effectuées.
- Audit n° 2, pentest de l'application : tests d'intrusion et simulations d'attaques, coût 30 000 €, durée 2 semaines.

## **Mois 15-18 : Tests internes**

### **Action 14 — Tests avec 1 000 utilisateurs pilotes**

Recrutement des testeurs : appel aux 1 000 Sentinelles actives issues de la Phase 1, avec un souci de diversité démographique (18-80 ans, urbains et ruraux, technophiles et non-technophiles).

Scénario de test : un vote fictif sur un sujet local — « Faut-il piétonniser le centre-ville de [votre ville] ? »

Processus : les testeurs téléchargent l'application, créent leur identité cryptographique, votent (Oui/Non/Blanc), vérifient leur vote, puis comparent les résultats pour simuler une convergence ou une divergence.

Collecte du feedback : questionnaire de satisfaction (Google Forms), bugs remontés (GitHub Issues), suggestions d'amélioration.

Métriques de succès :

- Taux de réussite à l'installation : supérieur à 95 %
- Taux de réussite du vote : supérieur à 90 %
- Taux de satisfaction : supérieur à 80 %
- Bugs critiques : zéro

C'est précisément à ce stade — un cercle fermé de testeurs, une question locale fictive, aucune valeur légale — que se situe le mois de l'élection présidentielle de 2027. Le mouvement citoyen sera alors à son pic de

visibilité politique (horizon 1) ; l'outil, lui, ne sera encore qu'en fin de mise au point (horizon 2).

## Budget Phase 2

Poste	Montant
Salaires de l'équipe (12 mois)	270 000 €
Audits de sécurité	80 000 €
Infrastructure (serveurs, cloud)	30 000 €
Juridique (conformité RGPD, etc.)	20 000 €
Communication (site, vidéos)	30 000 €
Tests utilisateurs (incentives)	10 000 €
Divers (imprévus, 10 %)	10 000 €
<b>TOTAL PHASE 2</b>	<b>450 000 €</b>

## Métriques de succès Phase 2

- Prototype fonctionnel (app iOS/Android + blockchain)
- 2 audits de sécurité passés avec succès
- 1 000 testeurs avec un taux de satisfaction supérieur à 80 %
- 0 bug critique non corrigé
- Code open-source publié sur GitHub
- Whitepaper technique publié

Si ces six objectifs sont atteints, passage en Phase 3.

---

## 4. PHASE 3 : Le Test Pilote (18-30 mois)

**Objectif** : prouver la viabilité en conditions réelles — localement.

**Livrable final** : un test grandeur nature dans une ville volontaire, avec 10 000 utilisateurs et une couverture médiatique nationale.

Cette phase s'ouvre après l'élection présidentielle de 2027 — c'est le début de l'horizon technique et légal. Le test porte sur un scrutin local (budget participatif ou référendum municipal), pas sur une élection nationale : il n'est donc pas contraint par le calendrier électoral national et peut se tenir dès que la ville partenaire organise son propre vote citoyen.

### Mois 18-21 : Identification de la ville pilote

#### Action 15 — Critères de sélection

Ville idéale : population entre 50 000 et 150 000 habitants, maire ouvert à l'innovation, population jeune et connectée, enjeu local mobilisateur (budget participatif, projet urbain).

Profil des villes cibles : villes de 50 000 à 150 000 habitants disposant déjà d'un budget participatif et d'une population jeune et connectée. Aucune ville n'est désignée ni contactée à ce stade : le choix se fera par appel à candidatures.

## **Action 16 — Partenariat avec la mairie**

Proposition à la mairie :

« Nous proposons de tester le ShadowVote lors de votre prochain vote citoyen (budget participatif, référendum local).

L'urne reste. Le ShadowVote s'ajoute.

Vous gagnez : une couverture médiatique nationale (innovation démocratique), une image de ville pionnière, un outil gratuit de vérification citoyenne.

Nous gagnons : un test en conditions réelles, une validation technique, une légitimité pour un futur déploiement national.

Risque : zéro. Le vote officiel reste valide. »

Engagements demandés à la mairie : autoriser l'usage du ShadowVote comme vote parallèle légal, communiquer sur l'expérimentation, fournir les données officielles pour comparaison, accueillir des ateliers d'initiation (bibliothèques, maisons de quartier).

## **Mois 21-24 : Préparation du test**

### **Action 17 — Campagne de communication locale**

Objectif : convaincre 10 000 citoyens de la ville d'utiliser le ShadowVote.

Outils : affiches dans la ville, flyers dans les boîtes aux lettres, ateliers d'initiation (mairies de quartier, bibliothèques), partenariats avec les associations locales, articles dans la presse locale.

Message :

« [Ville], ville pionnière de la démocratie vérifiable.

Le [date], votez sur [sujet] ET vérifiez votre vote avec le ShadowVote.

Ateliers gratuits : [dates et lieux].

|Plus d'infos : voir le livre ShadowVote. »

### **Action 18 — Formation des ambassadeurs locaux**

Recrutement : 50 ambassadeurs bénévoles, parmi les membres d'associations citoyennes, des étudiants engagés, des retraités actifs, des commerçants.

Formation, une journée : comprendre le ShadowVote, utiliser l'application, répondre aux objections, animer un atelier d'initiation.

Rôle : tenir des stands (marchés, gares), animer des ateliers (20 personnes par séance d'une heure), assister les personnes âgées pour l'installation de l'application.

### **Mois 24 : Le jour J**

#### **Action 19 — Vote test**

Déroulement : de 8h à 20h, vote classique et ShadowVote se déroulent en parallèle. Les citoyens votent normalement à l'urne. Ceux qui ont l'application (objectif : 10 000) votent aussi sur le ShadowVote.

Dispositif d'assistance : une hotline téléphonique (10 bénévoles) et des stands d'aide devant les bureaux de vote, pour le téléchargement de l'application sur place.

À 20h, dépouillement : l'urne officielle est dépouillée classiquement par les assesseurs ; les résultats du ShadowVote sont affichés en temps réel.

À 21h, comparaison publique lors d'une conférence de presse réunissant le maire de la ville, des représentants de ShadowVote et des journalistes nationaux : présentation des résultats de l'urne officielle, des résultats du ShadowVote, analyse des écarts, témoignages d'utilisateurs.

#### **Action 20 — Exploitation médiatique**

Objectif : une couverture nationale.

Si convergence (écart inférieur à 3 %), titre visé : « [Ville] prouve que le vote blockchain fonctionne : 99 % de convergence. » Message porté : « La technologie fonctionne. Il faut maintenant l'étendre, étape par étape. »

Si écart significatif (supérieur à 3 %), titre visé : « Vote à [Ville] : la blockchain révèle un écart de X % avec l'urne. » Message porté : « Ces outils de vérification sont indispensables. Imaginez si c'était une présidentielle. »

### **Mois 24-30 : Exploitation et bilan**

#### **Action 21 — Rapport public**

Livrable : un rapport de 100 pages couvrant la méthodologie du test, les résultats détaillés (convergence/divergence), l'analyse statistique, les retours utilisateurs (satisfaction, bugs) et des recommandations pour un déploiement national.

Diffusion : publication du rapport (version payante), envoi à tous les députés et sénateurs, présentation dans les think tanks, conférences universitaires.

## Action 22 — Lobbying politique

Cibles : députés de la commission des lois, sénateurs intéressés, ministère de l'Intérieur (direction des élections), Conseil constitutionnel (présentation informelle).

Message :

« Le test de [Ville] prouve que c'est faisable à l'échelle d'une ville. Nous proposons une loi encadrant une expérimentation nationale progressive : d'abord d'autres scrutins locaux volontaires, puis, une fois la loi votée et évaluée pendant deux ans, une extension aux élections nationales. Nous parlons ici, en toute transparence, de l'échéance de 2032 — municipales et présidentielle — et non de celle de 2027, déjà passée au moment où ce test a lieu. »

Ce message assume frontalement le calendrier : il ne s'agit plus de viser « les prochaines élections », formule vague qui aurait pu laisser croire à une adoption imminente, mais de nommer l'échéance réaliste, celle de l'horizon technique et légal défini en ouverture de ce chapitre.

## Budget Phase 3

Poste	Montant
Équipe (salaires, 12 mois)	300 000 €
Communication locale	50 000 €
Ateliers et événements	30 000 €
Infrastructure (scaling pour 10K utilisateurs)	50 000 €
Rapport et études	20 000 €
Lobbying (déplacements, réunions)	30 000 €
Divers	20 000 €
<b>TOTAL PHASE 3</b>	<b>500 000 €</b>

Financement : subventions UE (50 %), fondations (30 %), reliquat du crowdfunding de la Phase 2 (20 %).

## Métriques de succès Phase 3

- 10 000 utilisateurs testeurs

- Taux de participation supérieur à 15 % des inscrits de la ville
- Écart urne/blockchain inférieur à 3 %
- Couverture médiatique nationale (10 articles et plus)
- Rapport public publié
- 5 députés ou sénateurs engagés pour une proposition de loi

Si ces six objectifs sont atteints, passage en Phase 4.

---

## **5. PHASE 4 : Le Lobbying Politique (30-36+ mois)**

**Objectif :** obtenir un cadre légal pour un futur déploiement national, ou, à défaut, une adoption officielle partielle.

### **Mois 30-33 : Proposition de loi**

#### **Action 23 — Rédaction avec des parlementaires**

Travail avec 5 à 10 députés et sénateurs de différents bords, de façon strictement trans-partisane.

Titre de la loi : « Loi relative à l'expérimentation de la vérification citoyenne des scrutins par blockchain. »

Contenu, résumé :

- Article 1 : autorisation d'un vote parallèle sur blockchain lors des élections locales.
- Article 2 : le vote blockchain n'a aucune valeur légale, mais les résultats doivent être publiés.
- Article 3 : dans les bureaux participant à l'expérimentation, conservation des bulletins jusqu'à la publication des résultats du vote parallèle ; en cas de divergence supérieure à 3 points, obligation de recomptage.
- Article 4 : évaluation après deux ans. En cas de succès, extension aux élections nationales.

C'est cet article 4, avec ses deux années d'évaluation obligatoire, qui fixe l'horizon technique et légal évoqué en ouverture du chapitre à l'échéance de 2032, et non à celle de 2027.

#### **Action 24 — Campagne de soutien**

Objectif : faire pression sur les parlementaires.

Outils : relance de la pétition pour atteindre 500 000 signatures, emails automatisés aux députés, manifestation symbolique et pacifique devant l'Assemblée nationale, tribunes dans les journaux signées par des intellectuels et des scientifiques.

## **Mois 33-36+ : Vote de la loi**

**Scénario A — la loi passe.** Expérimentation officielle étendue lors des scrutins locaux suivants, budget de l'État alloué au déploiement, avec pour horizon l'échéance nationale de 2032. Victoire totale.

**Scénario B — la loi est bloquée.** L'État refuse d'adopter le ShadowVote officiellement. Mais si, entre-temps, 10 % des électeurs l'utilisent déjà de façon citoyenne et non officielle (voir chapitre 8), la pression morale est telle que les médias en parlent constamment, les candidats doivent se positionner, et le ShadowVote devient de facto un standard citoyen. Victoire partielle, mais réelle — et c'est précisément ce levier des 10 %, construit dès l'horizon politique de 2027, qui rend le Scénario B tenable même sans loi votée à temps.

---

## **6. Gestion des risques**

### **Risque 1 : attaque technique majeure**

Scénario : piratage de l'infrastructure, attaque DDoS massive, bug critique révélé publiquement.

Parade : audits de sécurité réguliers (tous les 6 mois), programme de bug bounty (récompenses pour signalement de failles), assurance cybersécurité. Plan de repli : suspension temporaire, correction, relance.

### **Risque 2 : interdiction légale**

Scénario : l'État déclare le ShadowVote illégal.

Parade : contestation juridique (liberté d'expression, CEDH), médiatisation massive (« L'État interdit de vérifier ? », traité comme un aveu), décentralisation internationale (serveurs hors de France).

### **Risque 3 : échec du crowdfunding**

Scénario : objectif non atteint (moins de 50 % de l'objectif visé, soit moins de 225 000 € collectés).

Parade : version allégée du prototype, un MVP réalisable avec 200 000 €, recherche de subventions complémentaires, étalement du développement (de 18 à 24 mois). Un tel retard repousserait d'autant l'horizon technique et légal, sans remettre en cause l'horizon politique de 2027, déjà atteint dès la Phase 1.

### **Risque 4 : divergence inexplicée lors du test**

Scénario : le test pilote montre un écart de 10 % avec l'urne, sans explication immédiate.

Parade : enquête approfondie (audit des deux systèmes), transparence totale (publication de toutes les données). Si l'erreur vient du ShadowVote : correction et nouveau test. Si l'erreur vient de l'urne : validation du ShadowVote.

### **Risque 5 : récupération politique hostile**

Scénario : un parti extrémiste déclare : « Nous soutenons le ShadowVote, votez pour nous. »

Parade : communication claire (« Le ShadowVote est trans-partisan »), refus de tout soutien partisan, encouragement de l'utilisation par tous les bords politiques, preuve vivante de neutralité.

---

## **7. Plan B : si le ShadowVote échoue**

### **Qu'est-ce qu'un « échec » ?**

- Échec technique : bug critique non résolu, piratage massif, technologie jugée non fiable.
- Échec politique : interdiction, censure, impossibilité de déployer.
- Échec citoyen : aucune adoption (moins de 1 % de la population testée utilisant réellement l'outil, un an après son lancement public).

### **Les leçons à tirer**

- Si échec technique : la blockchain n'était peut-être pas la bonne solution — trop complexe, trop chère. Il faut alors explorer d'autres technologies (vote par internet sécurisé, autres protocoles).
- Si échec politique : le système résiste plus qu'anticipé. Il faut alors continuer en mode « ombre » — usage citoyen non officiel, pression morale permanente.
- Si échec citoyen : le message n'a pas porté. Il faut alors revoir la communication, la pédagogie, la simplicité d'usage.

### **Les autres usages du protocole**

Si le ShadowVote — le vote électoral — échoue, le protocole blockchain peut servir à d'autres usages :

- Budgets participatifs locaux : les mairies utilisent la blockchain pour les votes sur des projets locaux, un terrain déjà moins sensible que les élections.
- Votes associatifs : les grandes associations et syndicats utilisent le protocole pour leurs élections internes.
- Preuves documentaires : évolution vers un JusticeChain, enregistrement de preuves, de documents, de témoignages.

Le ShadowVote n'est qu'une première application. Si elle échoue, la technologie reste. Les usages alternatifs peuvent réussir.

---

## **Conclusion du chapitre : le plan est prêt**

La feuille de route est claire, et elle assume désormais ses deux vitesses.

- Phase 1 (0-6 mois, horizon politique) : nous y sommes. Lancer le manifeste, la pétition, le collectif.
- Phase 2 (6-18 mois, horizon politique) : construire le prototype, lever les fonds, auditer. C'est cette phase qui traverse l'élection de 2027 — comme jalon de pression, pas comme mise en service.
- Phase 3 (18-30 mois, horizon technique et légal) : tester en conditions réelles, localement, et prouver la viabilité.
- Phase 4 (30-36+ mois, horizon technique et légal) : mener le lobbying politique, viser un cadre légal et, à l'échéance de 2032, un déploiement national ou une adoption citoyenne de facto.

Sur le plan budgétaire, l'ensemble est tenu de bout en bout : 18 000 € pour la Phase 1, 450 000 € pour la Phase 2, 500 000 € pour la Phase 3, avec six métriques de succès vérifiables à chaque étape. La gestion des risques couvre cinq scénarios avec, pour chacun, une parade concrète. Le Plan B couvre les trois formes d'échec — technique, politique, citoyen — et prévoit, si le vote électoral lui-même échoue, des usages alternatifs du protocole qui permettent à la technologie de survivre au projet.

Ce n'est plus un rêve. C'est un calendrier — un calendrier à deux horizons, assumé comme tel : la pression politique dès 2027, l'outil légalisé et déployé au cycle électoral suivant.

---

## **TRANSITION VERS LA PARTIE IV**

Dans le dernier chapitre (Partie IV), nous allons voir ce que VOUS pouvez faire MAINTENANT : les 5 actions concrètes, comment devenir Sentinelle, le serment.

Le plan existe. Il faut maintenant des bras pour l'exécuter.

Tournez la page. Votre révolution commence.

---

## **PARTIE IV**

### **L'APPEL — L'ACTION**

# CHAPITRE 10

## VOUS ÊTES LA RÉVOLUTION

« Il y a ceux qui regardent les choses comme elles sont et qui se demandent pourquoi. Moi, je les imagine comme elles pourraient être et je me dis : pourquoi pas ? »

— citation attribuée à George Bernard Shaw

---

### Introduction : le moment de vérité

Vous avez lu plus de cent pages.

Vous connaissez le diagnostic (Partie I). Vous comprenez la solution (Partie II). Vous avez intégré la philosophie (Partie III).

Maintenant, une question simple : qu'allez-vous faire ?

### Trois options s'offrent à vous

#### OPTION 1 — Refermer ce livre et ne rien faire

Vous êtes convaincu, mais vous attendez que « quelqu'un d'autre » lance le mouvement.

*Résultat* : rien ne change. Si les tendances actuelles se prolongent sans rupture, l'abstention pourrait avoisiner 35 % et la défiance envers les institutions 75 % d'ici cinq ans — une projection, pas un fait établi [estimation prospective]. Et vous vous direz : « J'aurais dû agir. »

#### OPTION 2 — Partager ce livre, mais rester spectateur

Vous achetez le livre. Vous partagez des extraits sur les réseaux sociaux. Vous recommandez l'achat à dix amis.

*Résultat* : une sympathie passive. Utile, mais insuffisante. Le mouvement a besoin d'acteurs, pas seulement de spectateurs.

#### OPTION 3 — Devenir Sentinelle

Vous agissez. Maintenant. Concrètement.

- Vous signez la pétition.
- Vous rejoignez le collectif.
- Vous convainquez trois personnes.
- Vous devenez un maillon actif de la révolution.

*Résultat* : le mouvement avance. Chaque Sentinelle compte. Vous êtes le changement.

Ce chapitre vous donne le mode d'emploi de l'Option 3.

---

## **1. Les cinq actions concrètes (à faire maintenant)**

### **ACTION 1 : signer la pétition — dès qu'elle sera en ligne**

**Pourquoi c'est important.** La pétition sera notre premier signal de force.

**Objectif visé :** 100 000 signatures en six mois à compter de son lancement.

Pourquoi 100 000 ?

- C'est le seuil médiatique (les journalistes commencent à couvrir).
- C'est le seuil politique : sur la plateforme officielle de pétitions du Sénat, une pétition qui recueille 100 000 signatures en six mois est transmise à la Conférence des présidents, qui peut décider d'un débat, d'une mission de contrôle ou d'une proposition de loi — sans y être obligée.
- C'est le seuil psychologique (le mouvement devient « sérieux »).

Une signature, ce sera un vote de confiance dans le projet.

**Où en est-on au moment où vous lisez ce livre.** Cette pétition n'existe pas encore : elle sera mise en ligne au lancement du mouvement, de préférence sur la plateforme officielle de pétitions du Sénat (ou, à défaut, sur une plateforme comme Change.org), avec un lien officiel qui sera annoncé avec la sortie de cet ouvrage. Rien d'autre ne doit être considéré comme le canal officiel tant que cette annonce n'a pas eu lieu — méfiez-vous de toute page qui prétendrait porter la pétition ShadowVote avant cette annonce.

### **Ce que vous pouvez faire dès maintenant, avant même son lancement**

1. Marquez ce livre, ou notez quelque part, votre intention de signer. 2. Parlez-en autour de vous (voir Action 3 et 4) — un mouvement qui compte des gens prêts à signer avant même l'ouverture de la pétition démarre plus vite. 3. Partagez le texte suggéré ci-dessous dès aujourd'hui, en l'adaptant : rien n'empêche de faire connaître l'idée avant que le mécanisme de signature existe.

#### **Texte de partage suggéré :**

J'ai lu "ShadowVote", et ça m'a secoué.

En 2026, on peut tracer un colis, mais pas un bulletin de vote. C'est absurde.

Le ShadowVote propose une solution : un vote citoyen parallèle sur blockchain, pour vérifier que notre voix compte vraiment. Le mouvement se lance — une pétition sera bientôt en ligne.

#NeCroisPlusVérifie #ShadowVote

*Temps nécessaire : 2 minutes.*

## **ACTION 2 : rejoindre le collectif — quand il ouvrira ses portes**

**Pourquoi c'est important.** Le ShadowVote n'est pas le projet d'une personne. C'est un mouvement horizontal de citoyens. Le collectif sera l'espace où vous poserez vos questions, échangerez avec d'autres Sentinelles, proposerez des idées et organiserez des actions locales. Plus nous serons, plus nous serons forts.

**Où en est-on au moment où vous lisez ce livre.** Ni le serveur Discord, ni le groupe Telegram, ni aucun autre espace collectif n'existent à l'heure où ce livre est publié — ils seront créés durant les tout premiers mois du mouvement (voir Chapitre 9, Phase 1). Leurs adresses exactes seront communiquées avec le lancement de la pétition (Action 1). Ne cherchez pas de groupe « ShadowVote France » avant cette annonce officielle.

### **Ce que vous pouvez faire dès maintenant**

1. Repérez ce livre ou son auteur (les canaux exacts seront précisés au lancement) pour être informé(e) de l'ouverture du collectif. 2. En attendant, commencez à identifier votre propre cercle : qui, autour de vous, serait prêt à rejoindre un groupe local dans votre ville dès son ouverture ? 3. Une fois le collectif ouvert, présentez-vous simplement : « Bonjour, je suis [prénom], [âge], [ville]. J'ai lu le manifeste et je suis convaincu(e). Comment puis-je aider ? »

*Temps nécessaire : 10 minutes le jour de l'ouverture, puis 30 minutes par semaine environ selon votre implication.*

## **ACTION 3 : partager le manifeste**

**Pourquoi c'est important.** Le manifeste ne vaut rien s'il reste sur une étagère. Il faut le propager. Chaque lecture, c'est un citoyen potentiellement éveillé.

**Objectif :** 10 000 lectures en six mois.

### **Comment faire**

- *Le livre papier :* si vous l'avez acheté, prêtez-le. Une règle simple : « Lis-le, puis passe-le à quelqu'un d'autre. » Un livre acheté peut ainsi toucher 5 à 10 lecteurs.

- *Les extraits numériques* : partagez des citations percutantes et incitez à l'achat, auprès de vos amis politisés, de votre famille, de vos collègues si le contexte s'y prête.
- *Les réseaux sociaux* :
- **X/Twitter** : « J'ai lu "ShadowVote" et ça m'a secoué. L'idée : un vote citoyen parallèle sur blockchain pour vérifier que nos bulletins comptent vraiment. Ça vaut le coup. #ShadowVote #NeCroisPlusVérifie »
- **Facebook** : un post plus long (environ 300 mots), avec une image du livre et un appel à la discussion : « Qu'en pensez-vous ? Est-ce qu'on devrait avoir le droit de vérifier notre vote ? »
- **LinkedIn** : une version professionnelle, axée innovation démocratique : « Intéressant manifeste sur l'usage de la blockchain pour restaurer la confiance électorale. Qu'en pensent les experts RH/Tech/Politique ici ? »
- **Instagram/TikTok** : une vidéo courte (30 à 60 secondes), vous avec le livre : « J'ai lu ce livre en trois heures. Il propose d'utiliser la blockchain pour qu'on puisse enfin vérifier que notre vote est bien compté. Je vous explique... »

*Temps nécessaire : 15 minutes de partage initial, puis le temps de répondre aux commentaires.*

## **ACTION 4 : convaincre trois personnes**

**Pourquoi trois ?** Si chaque lecteur convainc trois personnes, la croissance suit une logique exponentielle.

Étape de partage	Nombre de personnes	Calcul
Étape 0	1 lecteur	(vous)
Étape 1	3	$1 \times 3$
Étape 2	9	$3 \times 3$
Étape 3	27	$9 \times 3$
Étape 4	81	$27 \times 3$
Étape 5	243	$81 \times 3$
Étape 10	59 049	—

En dix étapes de partage successives, un lecteur devient, sur le papier, 59 000. Dans un **scénario optimiste maximal**, si mille lecteurs enclenchèrent ce cycle, on approcherait 59 millions de personnes touchées.

Ce calcul est un ordre de grandeur théorique, pas une prévision. En pratique, les recoupements de réseaux (on partage souvent aux mêmes personnes) et un taux de conversion réel bien plus faible que 100 % réduisent nettement ce chiffre. Il illustre la puissance potentielle du bouche-à-oreille structuré — il ne la garantit pas.

## Comment convaincre, sans être lourd

- *Le sceptique* : « Je sais que tu ne fais plus confiance au système électoral. Moi non plus. Mais j'ai lu un projet qui propose une solution concrète, pas juste des plaintes. Ça s'appelle le ShadowVote. Laisse-moi t'expliquer cinq minutes... » Arguments clés : vérifier son vote est un droit fondamental ; la technologie blockchain existe déjà et est mature ; le coût visé est très inférieur à celui de l'urne traditionnelle.
- *Le technophile* : « Tu connais la blockchain ? Imagine l'appliquer au vote : chaque bulletin enregistré de manière inaltérable, publique, vérifiable. C'est exactement ce que propose le ShadowVote. Regarde ce manifeste, c'est bien expliqué... » Arguments clés : décentralisation (pas de point unique de défaillance) ; code open-source et auditable ; ambition d'un coût de fonctionnement plus faible et d'une sécurité renforcée par rapport à l'urne.
- *Le pragmatique* : « Tu t'abstiens parce que tu penses que ça ne sert à rien. Je te comprends. Mais imagine pouvoir vérifier que ton vote compte vraiment. Ça changerait ta vision ? Le ShadowVote propose exactement ça... » Arguments clés : preuve cryptographique plutôt que foi aveugle ; convergence ou divergence des résultats, dans les deux cas on apprend quelque chose ; une action concrète, pas seulement de la théorie.

## Les trois erreurs à éviter

- Être péremptoire (« Si tu signes pas, t'es complice du système ! ») → ça braque. Restez pédagogue.
- Être trop technique (« Le hash SHA-256 garantit l'intégrité du Merkle tree... ») → vulgarisez, utilisez les analogies du livre.
- Forcer (« Allez, signe maintenant, devant moi ! ») → laissez réfléchir. Donnez les informations, laissez la personne décider.

*Temps nécessaire : trois conversations de 15 minutes, soit 45 minutes.*

Convaincre trois personnes, c'est le cœur du mouvement. Mais convaincre ne suffit pas toujours : certains d'entre vous ont des compétences à offrir. C'est l'objet de la cinquième action.

## ACTION 5 : contribuer selon vos compétences

Le ShadowVote a besoin de toutes les compétences, pas seulement de développeurs.

- **Développeur/développeuse** — compétences recherchées : blockchain (Solidity, Polygon), full-stack (React Native, Node.js), DevOps. Comment contribuer : code sur GitHub en open-source, revue de code entre pairs, tests et débogage.

- **Designer UX/UI** — compétences recherchées : conception d'applications mobiles, accessibilité (mode senior, malvoyants), identité visuelle. Comment contribuer : maquettes de la future application (Figma), infographies pédagogiques, vidéos explicatives.
- **Juriste/avocat(e)** — compétences recherchées : droit électoral, droit constitutionnel, RGPD et protection des données, droit des associations. Comment contribuer : analyse légale du protocole, rédaction des statuts de l'association, conseil compliance, défense en cas de contentieux.
- **Journaliste/communicant(e)** — compétences recherchées : relations presse, réseaux sociaux, rédaction, stratégie de communication. Comment contribuer : pitches médias, gestion des réseaux, communiqués de presse, organisation de conférences de presse.
- **Enseignant(e)/formateur(ice)** — compétences recherchées : pédagogie, vulgarisation scientifique, animation d'ateliers. Comment contribuer : ateliers d'initiation (bibliothèques, maisons de quartier), tutoriels vidéo, support téléphonique pour les seniors.
- **Retraité(e) actif(ve)** — compétences recherchées : temps disponible, réseau local, crédibilité intergénérationnelle. Comment contribuer : ambassadeur ou ambassadrice local(e), animation de stands (marchés, gares), témoignages.
- **Étudiant(e)** — compétences recherchées : énergie, maîtrise des réseaux sociaux, connexion avec la jeunesse. Comment contribuer : viralité sur les réseaux (TikTok, Instagram), organisation d'événements sur les campus, mobilisation de la jeunesse — la tranche d'âge qui s'abstient le plus massivement.
- **Citoyen lambda, vous !** — vous n'avez aucune compétence technique ? Ce n'est pas grave, vous pouvez quand même aider : distribuer des flyers téléchargeables, tenir un stand sur les marchés ou lors d'événements locaux, organiser une projection-débat, ou financer le mouvement dès qu'une structure légale aura été créée (dons de 10 à 100 €).

*Temps nécessaire : variable, de 5 à 20 heures par mois selon votre implication.*

---

## 2. Devenir Sentinelle : le mode d'emploi

**Qu'est-ce qu'une Sentinelle, pour rappel ?** Une Sentinelle est un citoyen qui utilise le ShadowVote, une fois disponible, pour vérifier son vote ; qui surveille la convergence ou la divergence des résultats ; qui alerte en cas d'anomalie détectée ; et qui contribue au mouvement à sa mesure. Pas de

hiérarchie. Pas de chef. Pas de carte de membre. Juste un engagement moral.

### Les cinq niveaux d'engagement — choisissez le vôtre

Niveau	Engagement	Temps	Impact	Vous êtes
1 — Sentinelle passive	Utiliser le ShadowVote pour vos propres votes, une fois l'outil disponible	5 min par élection	Vous augmentez la masse critique (objectif 10 %)	Le socle du mouvement
2 — Sentinelle partageuse	Niveau 1 + partage sur les réseaux + convaincre 3 personnes	1 h par mois	Vous multipliez le mouvement	Un amplificateur
3 — Sentinelle ambassadrice	Niveau 2 + animation d'ateliers + stands locaux	5 h par mois	Vous ancrez le mouvement localement	Un relais de terrain
4 — Sentinelle contributrice	Niveau 3 + contribution technique (code, design, juridique...)	10 h par mois	Vous construisez l'infrastructure	Un bâtisseur
5 — Sentinelle fondatrice	Niveau 4 + implication dans la gouvernance + financement significatif	20 h et plus par mois	Vous êtes au cœur du mouvement	Un pilier

Vous choisissez votre niveau. Tous sont utiles. Même les Sentinelles passives (niveau 1) sont essentielles.

### Le serment de la Sentinelle

Si vous devenez Sentinelle, voici le serment moral que vous prêtez :

**JE M'ENGAGE À VÉRIFIER.**

**Je ne crois plus sans preuve.**

Je ne délègue plus sans contrôle.

Je ne vote plus sans témoin.

Je suis une Sentinelle.

Je garde la preuve.

Je surveille les élections.

Je respecte la démocratie.

Non par défiance systématique,

Mais par responsabilité citoyenne.

Si le système converge, je le valide.

Si le système diverge, je l'alerte.

Je n'agis pas contre le gouvernement mais pour la démocratie.

Je suis pour la vérité.

Tout en restant fidèle à mes convictions, je sers la transparence.

Je ne suis pas seul(e).

Nous sommes des milliers.

Bientôt des millions.

Le Code ne remplacera pas la vertu,

Mais il rendra le mensonge impossible.

PLUS JAMAIS SANS PREUVE.

Ce serment n'est pas contraignant légalement. C'est un engagement personnel envers vous-même et envers la démocratie.

---

### 3. Les slogans du mouvement

Un mouvement a besoin de mots simples, frappants, mémorables. Voici les sept slogans du ShadowVote. Utilisez-les. Partagez-les.

1. « **Ne crois plus, vérifie.** » — Le passage de la foi aveugle à la preuve cryptographique. Usage : hashtag principal, #NeCroisPlusVérifie. 2. « **Ta voix est ta preuve.** » — Votre vote n'est plus une espérance, c'est une preuve mathématique. Usage : signature email, bio Twitter/Instagram. 3. «

**Chaque citoyen, une Sentinelle.** » — Le rôle actif et la responsabilité partagée. Usage : appel à rejoindre le mouvement. 4. « **Plus jamais de votes sans témoins.** » — L'exigence de transparence absolue. Usage : titre de tribune, pétition. 5. « **La transparence n'a pas d'ennemi.** » — Seuls ceux qui ont quelque chose à cacher refusent la transparence. Usage : argument face aux opposants au ShadowVote. 6. « **Le Code est libre, la Preuve est éternelle.** » — La garantie technologique (open-source, blockchain inaltérable). Usage : message technique pour les geeks. 7. « **Plus jamais sans preuve.** » — Le serment final. Le mantra du mouvement. Usage : conclusion de toute intervention publique.

**Hashtags à utiliser :** #ShadowVote #NeCroisPlusVérifie  
#TaVoixEstTaPreuve #PlusJamaisSansPreuve  
#ChaqueCitoyenUneSentinelle #LUrneEstMorte #Démocratie3Point0

---

## 4. Les événements à organiser

**Événement 1 — Le café citoyen.** Réunion informelle dans un café, 10 à 20 personnes, 1 h 30. Programme : 15 minutes de présentation du ShadowVote (vidéo ou slides), 30 minutes de débat et questions-réponses, 30 minutes d'actions concrètes (signer la pétition, découvrir la future application), 15 minutes de networking et d'échange de contacts. Fréquence : une fois par mois, dans chaque ville de plus de 50 000 habitants.

**Événement 2 — L'atelier d'initiation.** Formation pratique en bibliothèque ou maison de quartier, destinée en priorité aux seniors et aux personnes peu à l'aise avec le numérique. Durée : 2 heures. Programme : 30 minutes d'explication simple de la blockchain, sans jargon ; 30 minutes de démonstration du prototype de l'application sur écran géant — un prototype de démonstration, pas encore l'outil définitif ; 45 minutes de pratique guidée, où chacun s'exerce sur la maquette et simule les futures étapes d'utilisation ; 15 minutes de questions et de suivi. Matériel nécessaire : vidéoprojecteur, tablettes de prêt pour s'exercer sur la maquette (pour ceux qui n'ont pas de smartphone), et cinq à dix ambassadeurs bénévoles pour l'accompagnement individuel. Fréquence : une fois par trimestre.

**Événement 3 — La projection-débat.** Projection documentaire suivie d'un débat sur le ShadowVote, en cinéma associatif, centre culturel ou université. Durée : 2 h 30. Programme : 1 h 30 de projection d'un documentaire sur la démocratie numérique, 45 minutes de débat avec des intervenants (politologue, développeur blockchain, Sentinelle), 15 minutes d'appel à l'action (pétition, collectif). Fréquence : une fois par semestre.

**Événement 4 — Le hackathon ShadowVote.** 48 heures de développement intensif pour faire avancer le futur prototype de l'application, destiné aux développeurs, designers et étudiants en

informatique, sur un campus universitaire, dans un incubateur ou un FabLab. Programme : lancement et présentation des défis le vendredi soir ; développement en équipes de cinq à six personnes le samedi et le dimanche ; présentation des projets puis remise des prix le dimanche en fin de journée. Récompenses : badge « Contributeur ShadowVote », intégration du code retenu dans le futur prototype officiel, reconnaissance publique (nom dans les crédits). Fréquence : une fois par an, à partir de la Phase 2-3 du projet.

---

## 5. La timeline personnelle (vos six prochains mois)

Voici ce que vous pouvez faire dans les six prochains mois. Un calendrier concret, mois par mois.

### Mois 1

- *Semaine 1* : finir la lecture du manifeste, repérer les canaux officiels dès leur annonce (pétition, collectif).
- *Semaine 2* : partager le manifeste (réseaux sociaux + cinq amis), convaincre une première personne.
- *Semaine 3* : convaincre une deuxième personne, identifier votre compétence (dev, design, juridique, bénévole).
- *Semaine 4* : convaincre une troisième personne, signer la pétition et rejoindre le collectif dès leur ouverture.

### Mois 2-3

- Si vous êtes contributeur technique : rejoindre le futur dépôt de code ouvert dès son annonce, contribuer au code, au design ou au juridique.
- Si vous êtes ambassadeur : organiser un premier café citoyen (inviter dix personnes), proposer la création du groupe local de votre ville.
- Si vous êtes Sentinelle passive : suivre l'actualité du mouvement, partager les nouvelles sur vos réseaux.

### Mois 4-6 — phase de consolidation

- Participer à un événement local (atelier, projection-débat).
- Si possible, financer le projet dès qu'une structure légale aura été créée (10 à 100 €).
- Préparer le terrain pour la Phase 2 : le prototype.

Au bout de six mois, vous aurez signé la pétition, convaincu au moins trois personnes, contribué au mouvement à votre niveau, et fait partie des mille premières Sentinelles actives qui lancent la révolution. Vous aurez changé quelque chose.

---

## 6. Le kit de conversation (pour convaincre)

Vous allez rencontrer cinq types de réactions. Voici comment répondre.

**L'enthousiaste** — « Génial ! Comment je fais pour rejoindre ? » Réponse : « Super ! Pour l'instant, la pétition et le collectif ne sont pas encore ouverts — surveille l'annonce officielle du lancement. En attendant, voilà ce que tu peux déjà faire : partage le livre, et convaincs trois personnes de ton côté. » Puis : « Et si tu as des compétences — dev, design, communication —, garde-les au chaud : on cherchera des contributeurs dès l'ouverture. »

**Le sceptique** — « Mouais, bonne chance, mais l'État ne laissera jamais faire ça. » Réponse : « C'est exactement ce qu'on disait d'Uber : "Les taxis ne laisseront jamais faire." Et pourtant... Le ShadowVote ne demande pas la permission. C'est un vote citoyen parallèle et légal — il ne remplace pas le scrutin officiel, il le double pour le vérifier. Si 10 % des électeurs l'utilisent, l'État sera obligé de réagir. La question n'est pas "Est-ce que l'État va accepter ?" La question est "Combien de citoyens vont l'utiliser ?" Et ça, ça dépend de nous. De toi. De moi. »

**Le complotiste** — « Ah ouais ! C'est clair que les élections sont truquées ! Ils nous prennent pour des cons ! » Réponse : « Attention, le ShadowVote ne prétend pas que les élections sont truquées. On dit juste qu'on ne peut pas vérifier — et que cette impossibilité est inacceptable en 2026. Si le système est honnête, le ShadowVote le prouvera par la convergence des résultats. S'il y a des anomalies, le ShadowVote les révélera. Mais on ne part pas du principe que c'est truqué : on vérifie. Nuance importante. »

**Le technophobe** — « Moi et la technologie, c'est pas compatible. Je comprendrai jamais. » Réponse : « T'inquiète, tu n'auras pas besoin de comprendre la blockchain pour utiliser le ShadowVote. C'est comme ta carte bancaire : tu ne sais pas comment fonctionne la cryptographie, mais tu l'utilises quand même. L'application, une fois développée, sera pensée pour être ultra-simple — l'objectif est qu'elle tienne en trois gros boutons, accessible même à une personne peu familière du numérique. Et si tu galères, des ateliers d'aide gratuits seront organisés dans ta ville. »

**L'apolitique** — « Moi, la politique, j'en ai rien à faire. Qu'ils se démerdent. » Réponse : « Je comprends. Mais justement, le ShadowVote, ce n'est pas de la politique, c'est de la vérification. C'est comme vérifier ton relevé bancaire. Tu votes pour qui tu veux — ou tu ne votes pas, d'ailleurs. Mais si tu votes, tu mérites de savoir que ça compte vraiment. Ce n'est pas être pour un parti. C'est être pour la vérité. »

---

## 7. Le créateur qui s'efface : pourquoi je ne dirigerai pas ShadowVote

Avant de conclure, une question que beaucoup me posent mérite une réponse directe : qui dirigera ShadowVote ? Cette section explique pourquoi, malgré l'avoir conçu, je ne dirigerai pas le mouvement.

**Le paradoxe du fondateur.** Pour que ShadowVote réussisse, son créateur doit s'effacer.

**Raison 1 — Éviter la personnalisation.** ShadowVote ne doit appartenir à personne. Si je reste aux commandes, on parlera de « Nour-eddine Khaldi et son projet » plutôt que de l'idée elle-même ; les médias attaqueront ma personne plutôt que le fond ; et le mouvement risquera de mourir si je disparaissais. Solution : je deviens Sentinelle comme les autres, pas dirigeant.

**Raison 2 — La légitimité collective.** Une révolution démocratique ne peut être dirigée par un seul homme. Ce serait contradictoire avec nos valeurs : décentralisation contre centralisation, collectif contre individuel, transparence contre leadership opaque.

**Raison 3 — L'incompétence assumée.** Je ne suis pas compétent pour diriger ce mouvement. Techniquement, je ne sais pas coder une blockchain. En communication, je ne suis pas un marketeur. En organisation, je ne suis pas un manager d'équipe. Juridiquement, je ne suis pas avocat spécialiste. D'autres sont bien meilleurs que moi pour ces tâches.

**Raison 4 — La propriété collective.** Dès que vous adoptez ShadowVote, il devient autant vôtre que mien. J'ai écrit la première note de musique ; vous composez la symphonie ; l'orchestre nous appartient à tous.

### Mon rôle : créateur puis Sentinelle

- Phase 1 (Création) : j'écris le manifeste. Fait.
- Phase 2 (Transmission) : je lance le mouvement. En cours.
- Phase 3 (Effacement) : je deviens simple contributeur. Volontaire.

**La gouvernance post-lancement.** Qui va diriger ShadowVote ? La structure proposée s'appuie sur un conseil des Sentinelles (sept personnes élues), des équipes spécialisées (technique, communication, juridique), une assemblée générale annuelle, et des votes numériques pour les décisions importantes. Mon statut : membre consultatif, sans droit de veto.

**Pourquoi cette stratégie devrait fonctionner.** Elle devrait attirer de meilleurs talents, car les meilleurs ne s'engagent que s'ils peuvent prendre de vraies responsabilités. Elle devrait renforcer la résilience du mouvement : si je disparaissais, ShadowVote continue. Elle sert la crédibilité démocratique du projet : un mouvement pour la démocratie qui pratique la

démocratie. Et elle limite les attaques ad hominem : il est plus difficile d'attaquer un mouvement sans visage unique.

**L'engagement du créateur.** Je m'engage à participer comme Sentinelle active, à contribuer selon mes compétences (écriture, vision), à soutenir les équipes dirigeantes, à défendre l'idée dans les médias si nécessaire. Mais pas à diriger les équipes, prendre les décisions stratégiques, gérer les budgets, ou être le porte-parole officiel.

**Risques et réponses.** « Sans leader, le mouvement va se disperser » — des projets décentralisés comme Linux ou Wikipedia montrent que l'absence de dirigeant unique peut être une force plutôt qu'une faiblesse, à condition d'une gouvernance claire ; c'est cette voie que nous visons. « Les gens ne suivront que le créateur » — les vrais révolutionnaires suivent les idées, pas les hommes.

Je suis le père biologique de ShadowVote. Vous êtes ses parents adoptifs. Et comme tout bon parent adoptif, vous l'aimerez et le protégerez mieux que moi. C'est exactement ce que je souhaite.

Cette clarification faite, revenons à vous — car c'est vous, désormais, qui écrivez la suite.

---

## 8. Conclusion : l'acte fondateur

Chaque révolution citoyenne commence par un premier geste. Pour le mouvement des droits civiques : Rosa Parks refuse de céder sa place. Pour les Gilets jaunes : un premier rond-point occupé. Pour #MeToo : une parole qui, après des années de silence, finit par se répandre et se faire entendre.

Pour le ShadowVote, ce geste est double : signer la pétition, convaincre trois personnes. C'est tout.

Pas besoin de manifester. Pas besoin de casser. Pas besoin de crier. Juste signer, et convaincre.

**Le moment est venu.** Le diagnostic est posé (Partie I). La solution existe (Partie II). La stratégie est claire (Partie III). Le plan d'action est prêt (Chapitre 9). Il ne manque qu'une chose : vous.

**La promesse aux générations futures.** Demain, vos enfants vous demanderont : « Comment vous étiez sûrs que vos votes comptaient ? » Et vous pourrez répondre : « Parce que nous avons créé le ShadowVote. Et nous sommes devenus Sentinelles. »

**Le serment collectif.** C'est un serment collectif. Un pacte citoyen. Une promesse à la démocratie : « Plus jamais sans preuve. »

**L'appel.** Le Code va reprendre le pouvoir. Il est temps de mettre la puissance de la Preuve au service de la vérité.

Vous êtes la révolution. Elle commence maintenant.

---

## ANNEXE A — PROPRIÉTÉ INTELLECTUELLE

© 2026 Nour-eddine Khaldi. Tous droits réservés.

ShadowVote™ est la marque sous laquelle ce projet est développé et présenté au public. À la date de publication de cet ouvrage, ni le dépôt de cette marque, ni la structure légale, ni les canaux de contact officiels du mouvement n'ont encore été constitués ; leur mise en place progressive est prévue par l'auteur. Toute utilisation commerciale du nom ou du logo ShadowVote doit faire l'objet d'une autorisation préalable de l'auteur.

Les modalités de contact seront communiquées avec le lancement officiel du mouvement, dans les mois suivant la publication de ce livre.

## ANNEXE B — RÉFÉRENCES

Les données citées dans cet ouvrage s'appuient sur les catégories de sources suivantes :

- **Statistiques de participation et d'abstention électorale** — ministère de l'Intérieur (résultats officiels des scrutins français) ; Parlement européen (résultats définitifs des européennes 2024) ; US Census Bureau (participation aux États-Unis).
- **Indicateurs de confiance envers les institutions** — Cevipof (Sciences Po) / OpinionWay, Baromètre de la confiance politique, vague 2026.
- **Profil des abstentionnistes par âge** — enquêtes Ipsos (présidentielle 2022, législatives 2022, européennes 2024) et Ipsos-BVA (municipales 2026). Il s'agit de sondages : leurs résultats sont des estimations.
- **Coût des élections et machines à voter** — rapport d'information d'Hervé Marseille (commission des finances du Sénat, octobre 2015) ; réponse du ministère de l'Intérieur à la question écrite n° 03181 (JO Sénat, 26 décembre 2019) ; Insee, nombre d'inscrits sur les listes électorales (février 2026).
- **Textes et décisions juridiques** — Constitution (articles 3 et 89) ; Code électoral (articles L. 52-2, L. 63, L. 65, L. 68, L. 106, L. 113, L. 116, L. 117, R. 68, R. 119) ; Conseil d'État, 23 avril 2009 (Perpignan) et 8 juin 2009 (Corbeil-Essonnes) ; Conseil constitutionnel, proclamation des résultats de la présidentielle 2022 ; CNIL,

recommandation de 2019 sur le vote par Internet ; avis de l'ANSSI du 16 mars 2017.

- **Études académiques et documentation technique** — Centola, D., Becker, J., Brackbill, D., Baronchelli, A. (2018), « Experimental evidence for tipping points in social convention », *Science*, vol. 360, p. 1116-1119 ; M. Gladwell, *The Tipping Point* (2000) ; E. Rogers, *Diffusion of Innovations* (1962) ; documentation officielle des protocoles blockchain évoqués dans l'ouvrage.

Le lecteur souhaitant vérifier un chiffre précis est invité à se reporter aux publications correspondantes de ces organismes.

## **À PROPOS DE L'AUTEUR**

Nour-eddine Khaldi n'est ni élu, ni militant, ni diplômé en sciences politiques ou en économie. Il vit à Carpentras, dans le Vaucluse, et gagne sa vie sur les routes de France — comme des millions de Français qui se lèvent tôt et rentrent tard.

Ce qu'il a, c'est une habitude : se poser des questions, et poser celles que plus personne n'ose poser. La première a donné naissance à ce livre : « Pourquoi ne puis-je pas vérifier que mon vote a été compté ? » De cette interrogation est né ce projet : explorer, comprendre, proposer.

« Je ne suis qu'un passeur d'idées. L'avenir appartient à ceux qui les feront vivre. »