STRUCTURE

La preuve mathématique

Argumentaire complet à destination des avocats — répond à toutes les objections, dans l'ordre où elles se posent.

Le problème que vous connaissez mieux que quiconque

Votre cliente arrive avec 50 photos, des captures WhatsApp, des enregistrements audio, des photos de blessures. Et l'avocat adverse dit une seule phrase : « Ces preuves ont été fabriquées après coup. » Un seul doute — et le doute profite à l'accusé. Vous savez qu'elle dit la vérité, mais vous ne pouvez pas le prouver **mathématiquement** : démontrer que cette photo a été prise ce soir-là, à cette heure-là, et qu'elle n'a pas été modifiée depuis. **Jusqu'à maintenant.**

La preuve mathématique — comment ça fonctionne

Chose 1 — L'empreinte SHA-256 du fichier. Une fonction mathématique transforme n'importe quel fichier en une chaîne unique de 64 caractères. Si l'on modifie un seul pixel, une seule lettre, un seul caractère, l'empreinte devient totalement différente. Il est **mathématiquement impossible** de modifier un fichier sans que son empreinte SHA-256 change. Ce n'est pas une règle : c'est une loi mathématique.

Chose 2 — L'ancrage sur la blockchain Bitcoin. Structure envoie cette empreinte sur Bitcoin via le protocole open source OpenTimestamps. En moins d'une heure, elle est gravée dans un bloc Bitcoin — pour toujours — avec la date et l'heure exactes. Personne ne contrôle ce registre public mondial ; personne ne peut le modifier.

Ce que ça donne devant le tribunal

Scénario 1 — La photo de blessure

Frappée le 15 avril 2026 à 22h47, photo à 22h49, upload à 22h51, empreinte ancrée sur Bitcoin à 23h48. À l'audience, l'avocat adverse : « Cette photo a pu être prise n'importe quand et modifiée. »

> *« Monsieur le Président, voici la transaction Bitcoin publique confirmée le 15 avril 2026 à 23h48. Elle contient l'empreinte SHA-256 de cette photo. Vérifiez vous-même sur opentimestamps.org. Si la photo avait été modifiée d'un seul pixel, l'empreinte serait différente. Elle ne l'est pas. C'est une certitude mathématique — pas une opinion. »*

Scénario 2 — Le message WhatsApp

Message menaçant « Tu vas le regretter » le 3 juin 2026 à 02h35, capture à 02h36, ancrage à 03h21. « Cette capture existait le 3 juin à 02h36. Si un seul caractère — même l'heure affichée — avait été modifié, l'empreinte serait différente. Elle ne l'est pas. Ce message a été envoyé. C'est mathématiquement établi. »

Scénario 3 — L'enregistrement audio

45 secondes d'audio uploadées immédiatement, empreinte ancrée sur Bitcoin. « Si un seul mot avait été ajouté, supprimé ou modifié depuis, l'empreinte serait différente. Ce que vous entendez aujourd'hui est exactement ce qui a été enregistré ce soir-là. »

Les questions que vous allez poser

1. « Les juges connaissent et acceptent-ils cela ? »

Oui, et de plus en plus. En France, la **loi PACTE (22 mai 2019)** reconnaît les inscriptions dans des dispositifs d'enregistrement partagés (blockchain) comme moyen de preuve. Le **Règlement eIDAS (UE**

910/2014) reconnaît l'horodatage électronique comme moyen de preuve dans tous les États membres (art. 41 : l'effet juridique d'un horodatage qualifié ne peut être refusé). En Espagne, la **Ley 59/2003** et la jurisprudence admettent les preuves numériques horodatées. Aux États-Unis, plusieurs États (Vermont, Delaware, Wyoming…) reconnaissent les enregistrements blockchain. Surtout, les juges apprécient l'incontestable : un fait mathématique simplifie leur décision.

2. « L'avocat adverse va contester la blockchain. »

On peut contester une expertise, un témoignage, une photo. On ne conteste pas Bitcoin : modifier une transaction exigerait de contrôler simultanément plus de 51 % de la puissance de calcul de millions de machines réparties dans le monde. Aucun tribunal n'accepterait sérieusement cet argument.

3. « Et si c'est Structure qui a fabriqué les preuves ? »

C'est la seule objection sérieuse — et elle a une réponse sérieuse. Structure n'ancre pas les fichiers, mais leurs **empreintes**, calculées à partir du fichier original sur le téléphone au moment de l'upload, puis transmises à **OpenTimestamps** (protocole open source indépendant, maintenu par Peter Todd, utilisé par notaires, journalistes et tribunaux). Structure n'a aucune capacité à modifier une transaction déjà inscrite sur Bitcoin — personne ne l'a. La preuve n'est pas « Structure dit que ce fichier est authentique » mais « **Bitcoin prouve que ce fichier existait à cette date** ».

4. « Est-ce que ça remplace une expertise judiciaire ? »

Dans la plupart des cas, ça la rend inutile. Une expertise coûte 500 à 3 000 €, prend 3 à 6 mois, peut être contestée par une contre-expertise. Le certificat Bitcoin est gratuit, immédiat, non contestable par contre-expertise, sans délai procédural. Quand une expertise reste nécessaire (analyse du contenu d'un enregistrement), le certificat la **complète** : il prouve que le fichier soumis à l'expert est identique à l'original capturé le soir de l'incident.

5. « Ma cliente peut-elle documenter avant de décider de porter plainte ? »

C'est un atout majeur. Chaque incident et chaque preuve est ancré sur Bitcoin au moment où ça se passe. Quand elle décide de vous consulter — 3 semaines ou 8 mois plus tard — le dossier est constitué et les preuves sont datées du jour exact des faits, pas du jour de la plainte. Une différence fondamentale pour la procédure.

Ce que ça change pour votre pratique

Avant Structure : 3 à 5 heures pour trier des photos sans contexte, reconstituer une chronologie de mémoire, numéroter les pièces, rédiger l'exposé des faits — pour un dossier fragilisable par « Elle a tout inventé ».

Avec Structure, vous ouvrez le dossier et vous avez immédiatement :

- Chronologie certifiée de tous les incidents
- Pièces indexées avec leur certificat Bitcoin
- Exposé des faits rédigé par l'IA en langage juridique
- Projet de conclusions pré-rempli
- Stratégie d'audition avec questions ciblées
- Certificats Bitcoin pour chaque preuve

Et quand l'adversaire dit « Elle a tout inventé », vous montrez les certificats et répondez : « Prouvez-le mathématiquement. » Il ne peut pas.

En résumé

- Structure calcule l'empreinte mathématique unique de chaque preuve au moment de la capture.
- Cette empreinte est ancrée sur Bitcoin, le registre public le plus sécurisé jamais créé, dans l'heure.
- Elle est vérifiable publiquement par quiconque — vous, le juge, l'adversaire — en temps réel à l'audience.
- La moindre modification (un pixel, un caractère, une milliseconde) change l'empreinte : la falsification est détectée.
- Deux impossibilités mathématiques combinées (modifier un fichier sans changer son empreinte ; modifier une transaction Bitcoin) rendent la preuve incontestable.
- Conforme au Règlement eIDAS, à la loi PACTE et à la loi espagnole sur la signature électronique.

> *« La justice ne devrait pas dépendre de qui parle le mieux. Elle devrait dépendre de qui prouve mathématiquement. »*