

[Pour accéder au GitHub](#)  
[cliquer ici](#)



---

# WHITEPAPER

---

V1



27 JUILLET 2021

SAV-DOC  
Incubateur Alyra

## Table des matières

Préambule .....	2
Problématique.....	2
Vision projet .....	3
Avantages et bénéfices face à l'existant .....	3
Les fonctionnalités .....	4
Cas d'usage.....	4
Matrice de flux .....	6
Diagramme de Flux de SAV-Doc.....	6
Explication du fonctionnement Technique .....	8
Ecosystème de déploiement .....	8
Spécifications fonctionnelles.....	8
SmartContract .....	10
Gestion des risques d'utilisation .....	10
L'équipe projet .....	11
Le POC .....	11

## Préambule

L'ensemble de nos interactions sociales reposent sur des justifications de nos droits au travers de divers documents émis par diverses entités et signatures permettant de signifier notre accord / engagement.

Justifier de manière rapide et irréfutable notre bonne parole est souvent complexe due au fait de devoir recourir à différents tiers de confiance pour prouver que nous sommes bien dans notre droit.

## Problématique

La principale problématique réside dans le fait d'être dépendant de tiers de confiance et de leur intégrité pour faire valoir nos droits. Que ce soit pour justifier l'authenticité/intégrité d'un document, pour le sécuriser ou tout simplement pour le transmettre et en assurer le suivi.

Plus une procédure de justification fait appel à des tiers pour aboutir, plus le facteur risque augmente mais également le facteur temps surtout dans le cas où il n'existe pas de synchronisation métier entre les différents tiers requis.

Tout cela a pour conséquence d'alourdir la charge de nos procédures de justification et implicitement leur coût, ce qui par ricochet crée des inégalités à faire valoir ses droits. Autrement dit, les plus démunis sont plus facilement découragés de faire valoir leur droit au vu du casse-tête administratif associé à son coût financier.



## Vision projet

Permettre à tout le monde et ce sans tiers de confiance de :

- Sauvegarder et transmettre de manière sécurisée et confidentielle un document
- Signer et solliciter une signature
- Vérifier l'intégrité d'un document ainsi que l'ensemble des informations qui y sont rattachées (émetteur, propriétaire, signataire)

D'un point de vue global cela permet à chaque protagoniste (émetteur, récepteur, signataire) de prouver de manière publique le respect de ses engagements contractuels ou de son droit. Cela permet d'assurer un cycle de vérification « documentaire » public tout en préservant la confidentialité de la donnée.



## Avantages et bénéfices face à l'existant

Il existe déjà des solutions sur le marché que ce soit en version centralisée ou s'appuyant sur la blockchain, mais aucune solution ne propose l'ensemble de ces services (stockage, e-signature, envoi, vérification) de manière 100% décentralisée dans la plupart des cas on trouve au mieux des solutions hybrides.

SAV-Doc permet la transparence du traitement tout en assurant la confidentialité du contenu et cela sans aucun tiers de confiance.

Notre système de gestion documentaire dématérialisé et complètement décentralisé procure les bénéfices suivants :

- Suppression des intermédiaires : réduction des coûts et délais de traitement
- Suppression de la gestion papier : réduction l'espace physique de stockage et suppression du risque de détérioration
- Autonomie dans la capacité à se justifier : simplification des procédures de vérification



## Les fonctionnalités

SAV-DOC vous permet :

- De sauvegarder un document sous forme de NFT dont vous seul aurez l'accès (aucun tiers de confiance entre vous et vos documents).
- De transmettre un document de manière sécurisée sous forme de NFT. Seul votre destinataire pourra consulter le document (aucun tiers ne pourra y avoir accès)
- De solliciter la signature numérique d'un document
- De signer un document numériquement avec la possibilité d'en garder une copie sécurisée
- Vérifier les signatures d'un document (l'intégrité des documents est assurée par le NFT)
- Vérifier qui possède un document ou l'une de ses copies et qui en est l'émetteur

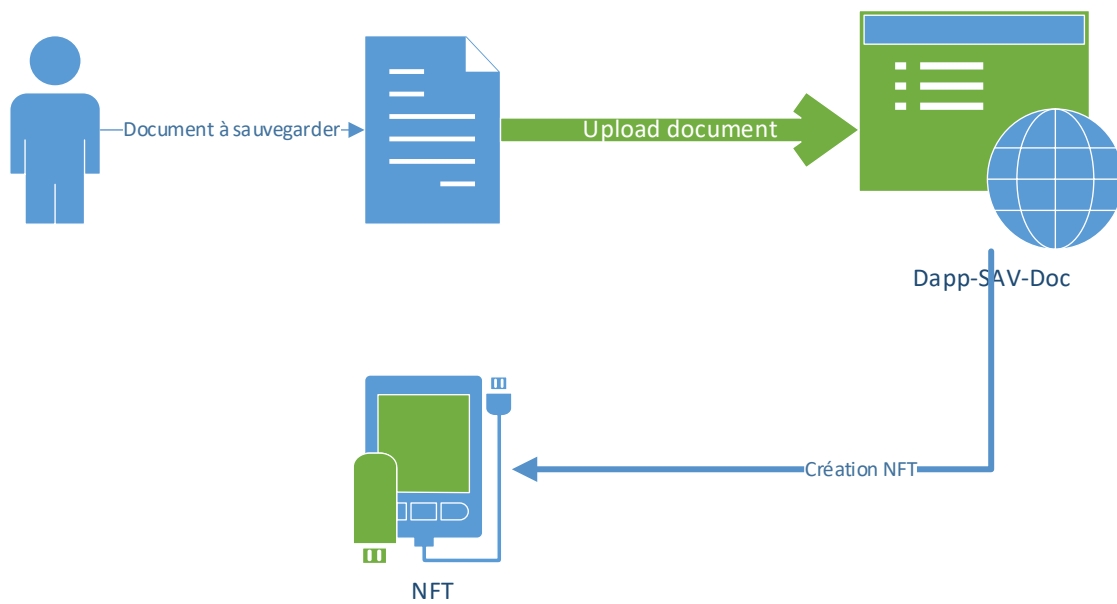
## Cas d'usage

SAV-Doc vous permet de stocker, envoyer et signer n'importe quel type de document (pdf, jpeg, mp4 etc...) il s'adresse aussi bien aux particuliers qu'aux entreprises et aspire à servir de référence pour les services publics dans le cadre de l'[EBSI](#).

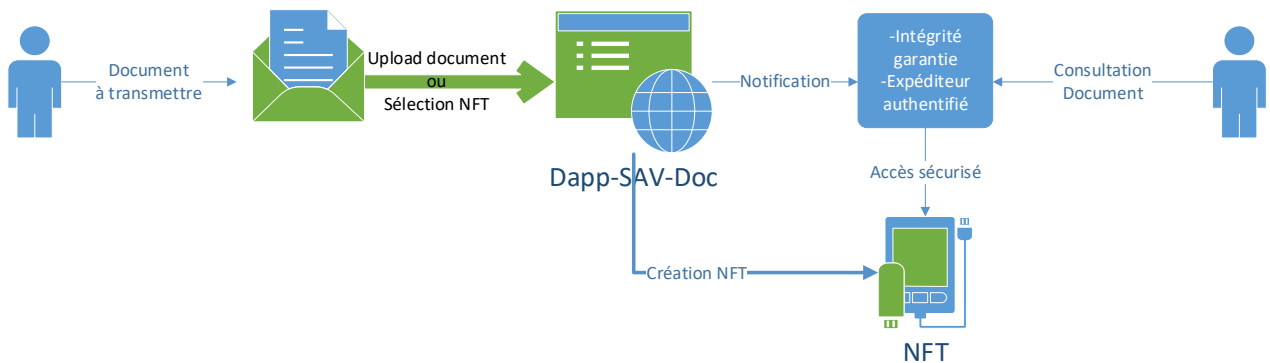
Exemple de cas d'usage pratique :

- Vous avez une photo de famille qui n'a pas de prix à vos yeux, vous en effectuez une sauvegarde sécurisée à travers le temps.
- Vous devez envoyer un devis à une société qui a la réputation de modifier les documents avant de les signer, vous envoyez un document non modifiable qui sera horodaté avec expéditeur et destinataire.
- Vous devez faire signer un bon de commande à une entreprise ayant la réputation de mauvais payeur, vous demandez une signature qui ne pourra pas être contestée et rattachée à un document dont l'intégrité ne peut pas être réfutée par le signataire.
- Un organisme doit vous transmettre une attestation dont il est reconnu garant par la loi, il l'authentifie comme étant émetteur empêchant sa réfutabilité et vous identifie comme propriétaire/titulaire (exemple : preuve de vaccination au frontière, attestation de preuve de travail/formation, délivrance de permis, titre, etc...).

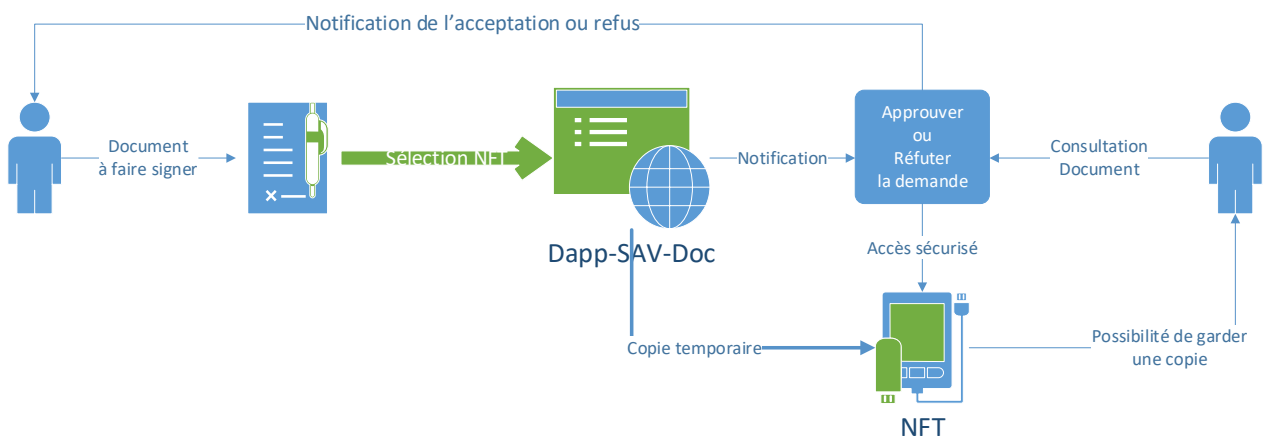
- Sauvegarder un document



- Envoyer/partager un document en garantissant son intégrité et sa provenance



- Signer un document numériquement



## Matrice de flux

### Enregistrement sur l'application

Installation des composants nécessaires (métamask...) → validation demande inscription → création mot de passe maître pour accéder à l'ensemble des documents sécurisés



### Sauvegarde / transfert



Upload d'un document numérique → génération d'un mot de passe pour protéger le document → choisir « à transmettre » ou « à sauvegarder », chiffrement du contenu au travers d'un NFT dont la lecture du contenu ne pourra être effectuée que par le propriétaire du NFT

### Signature / demande de signature



Signature d'un document que l'on possède → choix du document → signature.

Demande de signature d'un document par un tiers → transmission d'une copie temporaire + notification au travers de l'application au destinataire → possibilité de garder une copie → accepter ou non de signer

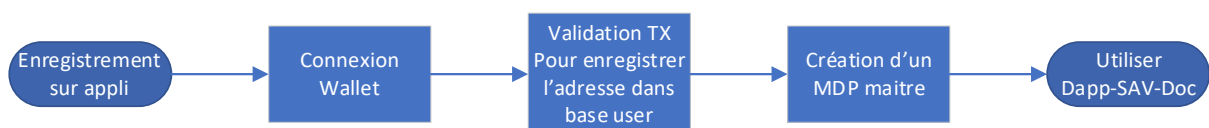
### Vérification

A partir de l'ID d'un document il est possible à n'importe qui de vérifier l'émetteur, les propriétaires et signataires.

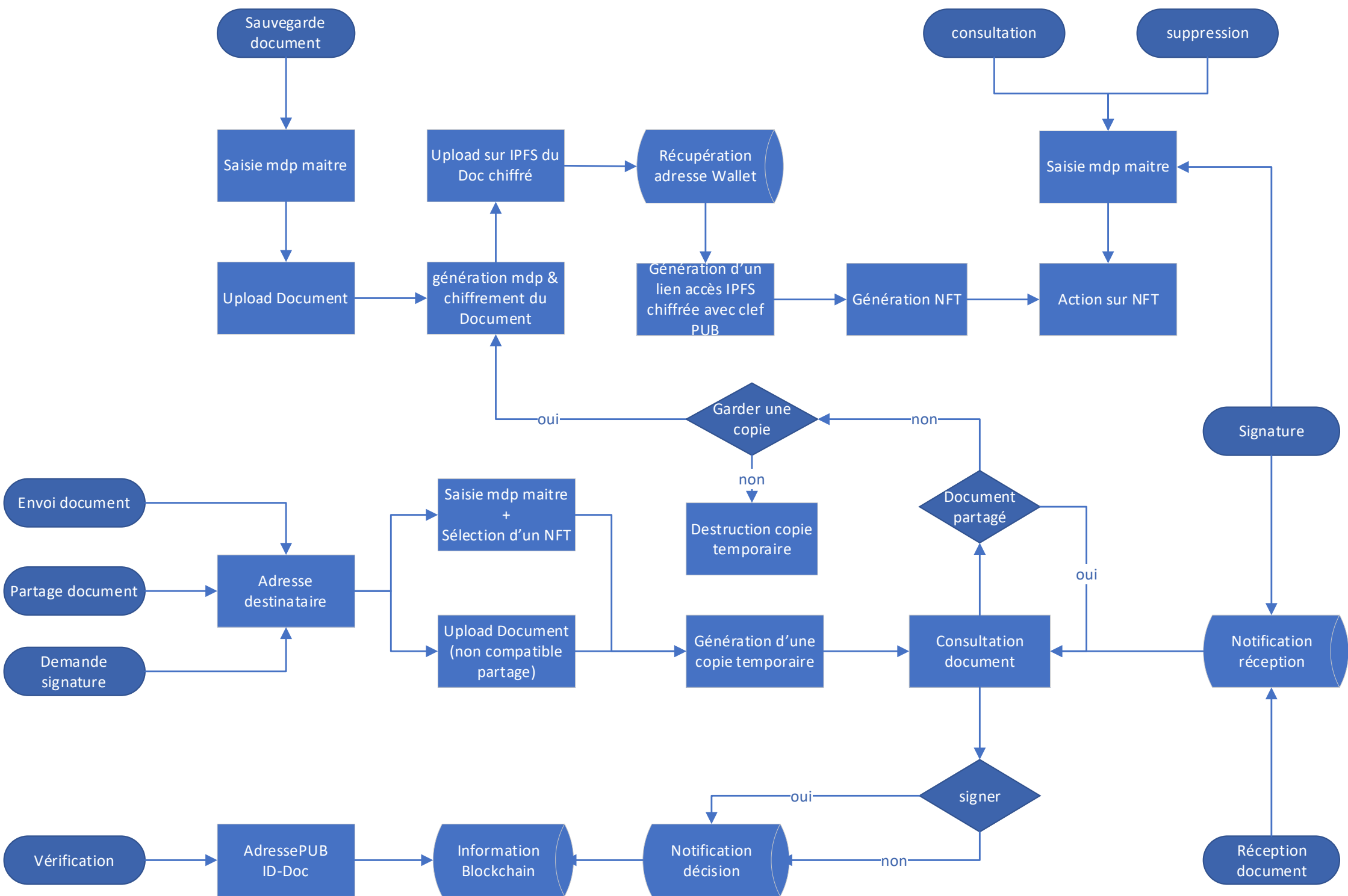


## Diagramme de Flux de SAV-Doc

### Enregistrement



### Utilisation





## Explication du fonctionnement Technique

L'ensemble des sources est disponible à cette adresse <https://github.com/asteux/SAV-Doc>

### Ecosystème de déploiement

Nous avons choisi la blockchain Ethereum pour initier notre POC comme demandé par notre incubateur de projet l'école Alyra, il est effectivement important de souligner la prédominance du langage solidity dans l'univers des Dapp et au-delà de cet aspect Ethereum est la Blockchain Turing complet disposant du plus haut niveau de décentralisation. Néanmoins son succès en fait également sa faiblesse, de nombreuses Dapp se développent dessus mais son nombre de transactions journalières restent pour le moment bridées à 1,5Millions, ce qui amène en cas de sur-sollicitation de cette dernière des frais de gas élevés.

Notre volume de transaction étant amené à devenir important sur notre application, le coût d'utilisation pour les utilisateurs risque de ne plus s'avérer bénéfique. Nous étudions donc sur quelle blockchain migrer pour notre phase de production, les pistes actuelles sont Polygon avec 5Milliard de TX/jour, Solana avec 17milliard de TX/jour et enfin la solution actuellement en cours de déploiement pour l'[EBSI](#), une version hybride de blockchain publique et privée s'appuyant sur [HyperLedger et BESU](#).

### Spécifications fonctionnelles

**Enregistrement sur l'application** : Pour utiliser l'application il est nécessaire de s'enregistrer afin d'obtenir la clef publique (différente de l'adresse publique) et de l'associer à un mot de passe (choisi par l'utilisateur) c'est grâce à ces 2 éléments que l'on peut générer le coffre-fort numérique qui protégera vos documents.



**Mot de passe pour chiffrement** : Afin d'assurer un bon niveau de chiffrement pour les documents l'application génère de manière automatique pour chaque document un mot de passe qui est lui-même chiffré avec le mot de passe maître. L'utilisateur n'a ainsi besoin que de retenir son mot de passe maître et est assuré d'avoir un mot de passe solide pour chiffrer ses documents. Le mot de passe maître est chiffré avec la clé publique puis le hash résultant de cette opération est stocké onchain.

**Stockage document :** Pour stocker le document nous faisons appel à la technologie IPFS (système de stockage décentralisé en P2P). Les documents sont uploadés en étant chiffrés par le mot de passe autogénéré dans le cas d'une sauvegarde et temporairement en clair pour un envoi.

**Accès document :** L'accès au document stocké sur IPFS se fait au travers d'un lien, pour renforcer la protection ce lien d'accès est chiffré avec la clef publique du propriétaire.

**Création du NFT :** pour « matérialiser » ce document sur la blockchain nous utilisons un NFT de type ERC-721, ce NFT contient le lien chiffré d'accès au document. Les attributs du NFT sont les suivants : ID-unique, créateur, propriétaire, type (original/copie-ID-original), signataire (Adresse-PUB-acceptation/refus)

**Demande de signature :** pour demander une signature à un tiers celui-ci doit être également enregistré sur l'application (nécessité d'avoir sa clef publique associée à son adresse publique pour le chiffrement de la copie temporaire). On sélectionne le document souhaité puis on renseigne l'adresse-PUB du destinataire, une notification au travers de l'application sera alors adressée au destinataire avec une copie temporaire du document.

**Copie temporaire :** La génération d'une copie temporaire à destination d'un signataire s'effectue en déchiffrant (grâce au mot de passe maître) le document souhaité, celui-ci est alors chargé dans le cache du navigateur depuis lequel l'application va le récupérer pour l'uploader (en clair) sur IPFS, néanmoins le lien d'accès sera lui chiffré avec la clef-PUB du destinataire afin d'en garantir la confidentialité.

**Envoi d'un document :** Comme pour la demande de signature il faut que le destinataire soit enregistré sur l'application, on upload le document qui est chargé sur IPFS (en clair) et le lien d'accès est ensuite chiffré avec l'adresse-PUB du destinataire, à réception le destinataire pourra effectuer le chiffrement du contenu sur IPFS (grâce à son mot de passe maître) ou tout simplement le supprimer après consultation. L'action de chiffrer le contenu sur IPFS remplacera le NFT reçu. Le principe est le suivant : on conserve les attributs de NFT reçu, toutefois le lien d'accès IPFS change suite au chiffrement.

**Partage d'un document :** identique à l'envoi d'un document mais pas d'option de conservation d'une copie.

**Suppression d'un NFT :** lors du choix de suppression d'un NFT, le contenu sur IPFS est supprimé, puis le NFT envoyé vers l'adresse 0000 cela rend impossible son accès, ce principe est autrement appelé « BURN »

## SmartContract

- AccountManager : permet de gérer les comptes utilisateurs
  - o 0x278A35Bf8a7D9d2F0aE3cfb0D68b8636c46b561d
- DocManager : permet de gérer les documents
  - o 0xCC94F27c020D52a11206FF658818343650E993Bd
- SaveDoc : est le contrat principal, permet de gérer les documents
  - o 0x0FD43c7Cf30737aC6eaCc53519f282f210cCd549
- SaveDocToken : permet de gérer les NFT
  - o 0xFC98bFee4540a4B9B8f96b0b6CEFaEf3ba8A0bF7

## Gestion des risques d'utilisation

Le fonctionnement d'une blockchain et son utilisation sont encore loin d'être popularisés (risque majeur identifié à l'adoption de notre solution). Pour amoindrir cette problématique un ensemble de tutos sera mis à disposition pour accompagner l'utilisateur dans l'installation des composants nécessaires ainsi que pour vulgariser le fonctionnement de la Blockchain. Pour faire comprendre la notion de coût d'utilisation de la blockchain (le GAS) nous afficherons le solde du wallet sous forme de réserve d'encre numérique en expliquant que c'est grâce à elle qu'il est possible de rendre immuable dans le temps l'ensemble des documents et signatures.







Nous mettrons à disposition un support par mail et un chat bot afin de répondre au plus vite aux interrogations de nos utilisateurs en les orientant vers la documentation appropriée.

Dans un souci d'optimisation de la sécurité, l'intégralité des smartcontract sera auditée avant d'être déployée en production. Le risque 0 ne pouvant être atteint nous étudierons la possibilité de proposer aux utilisateurs la souscription d'une assurance au travers d'un partenaire, à noter que Certik peut assurer le périmètre du code qu'il a audité.

Afin de renforcer le chiffrement des mots de passes générés (puis chiffrés avec le mot de passe maître) une contrainte de mot de passe fort sera mise en place pour le mot de passe maître demandé à l'enregistrement (12 caractères, majuscule, minuscule, chiffre, caractères spéciaux). Les utilisateurs étant habitués aux gestions centralisées et à la possibilité d'oublier leur mot de passe puis d'en demander un nouveau, nous ajouterons également un avertissement explicite sur le fait que nous ne pourrions pas effectuer ce genre d'opération du fait de la nature décentralisée de notre projet. Afin d'accompagner les utilisateurs dans la gestion d'un mot de passe fort ainsi que le moyen de s'en souvenir nous mettrons à leur disposition un lien vers un outil de la CNIL très bien conçu pour cet exercice <https://www.cnil.fr/fr/generer-un-mot-de-passe-solide> ainsi que des tutos sur l'utilisation d'outils spécialisés comme [KeePass](#).

Un autre élément de sécurité est trop souvent négligé car dépendant d'un facteur humain, celui des arnaques. Notre application offrant la possibilité aux institutions de valider des documents, une fraude portant sur ce point serait excessivement préjudiciable pour la promotion des outils Blockchain dans notre quotidien, nous mettrons donc en place un processus de certification interne pour les administrations en attendant qu'un processus d'identification validée par les autorités soit mis en place.

## L'équipe projet

 <p>Oumar TRAORE : Lead DEV Front</p>	 <p>Alexandre STEUX : ProductOwner ; Business Développeur</p>
 <p>Jean-Gabriel GNAHOUA : Lead DEV Back</p>	 <p>Corine GRESSION : ScrumMaster ; Project Manager</p>

Notre projet vous intéresse, vous souhaitez participer :

- Au développement et revue du code : GitHub <https://github.com/asteux/SAV-Doc>
- D'une autre manière ou pour toute question, merci de prendre contact avec notre incubateur Alyra : [bonjour@alyra.fr](mailto:bonjour@alyra.fr)



## Le POC

Pour tester et découvrir les fonctionnalités de notre POC munissez-vous de votre navigateur préféré et d'un wallet Metamask sur le réseau de test « Ropsten » assurez-vous d'avoir de l'ETH ([pour en obtenir gratuitement cliquer ici](#)) rendez-vous ensuite à cette adresse : <https://sav-doc.herokuapp.com>

