source

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

Répartition des fonctions 9

Expérience utilisateur 10

Préambule

L'ensemble de nos interactions sociale 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 confiances 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 les 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 cout, ce qui par ricoché 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 coup financier.

Vision projet

Permettre à n'importe qui et ce sans tiers de confiance de :

- Sauvegarder et transmettre de manière sécurisé 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)

Cela permet d'un point de vue global d'assurer à chaque protagoniste (émetteur, récepteur, signataire) de prouver de manière public le non-respect éventuel d'un tiers vis-à-vis de ses engagements contractuels. Cela permet d'assurer un cycle de vérification « documentaire » publique 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 centralisé ou s'appuyant sur la blockchain, mais aucune solution ne propose l'ensemble de ces services (stockage, e-signature, envoi, vérification) de manière 100% décentralisé 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 system de gestion documentaire dématérialisé et complètement décentralisé procure les bénéfices suivants :

- Suppression des intermédiaires : réduction des couts et délais de traitement
- Suppression de la gestion papier : réduction espace physique de stockage et supprime le 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 sécurisé 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 public dans le cadre de l'EBSI.

Exemple de cas d'usage pratique :

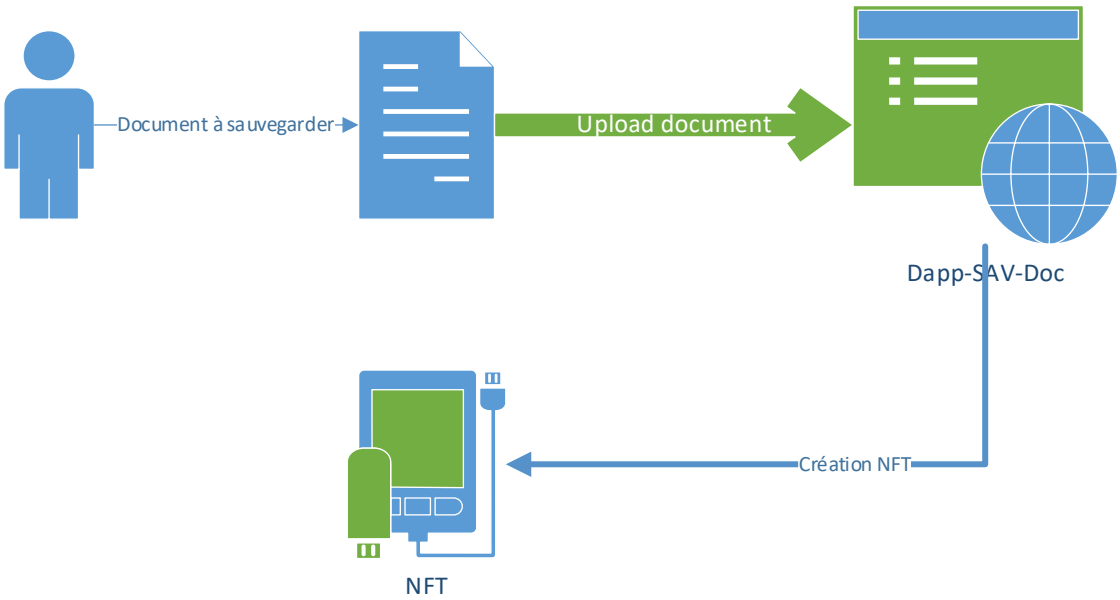
- Vous avez une photo de famille qui n'a pas de prix à vos yeux, vous en effectué une sauvegarde sécurisée à travers le temps.

- Vous devez envoyer un devis à une société qui à la réputation de modifier les documents avant de les signer, vous envoyez un document non modifiable qui sera horodaté avec expéditeur et destinataire.

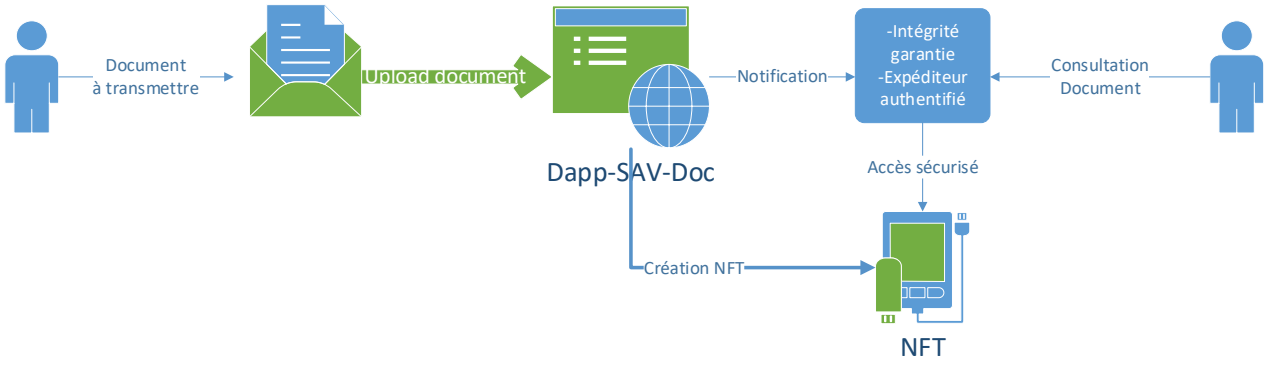
- Vous devez faire signer un bon de commande à une entreprise ayant la réputation de mauvais payeur, vous demandez une signature qui ne pourra pas être contestée et rattaché à un document dont l'intégrité ne peut pas être réfutée par le signataire.

- Un organisme doit vous transmettre une attestation dont elle est reconnue garante par la loi, elle l'authentifie comme étant émettrice 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…) .

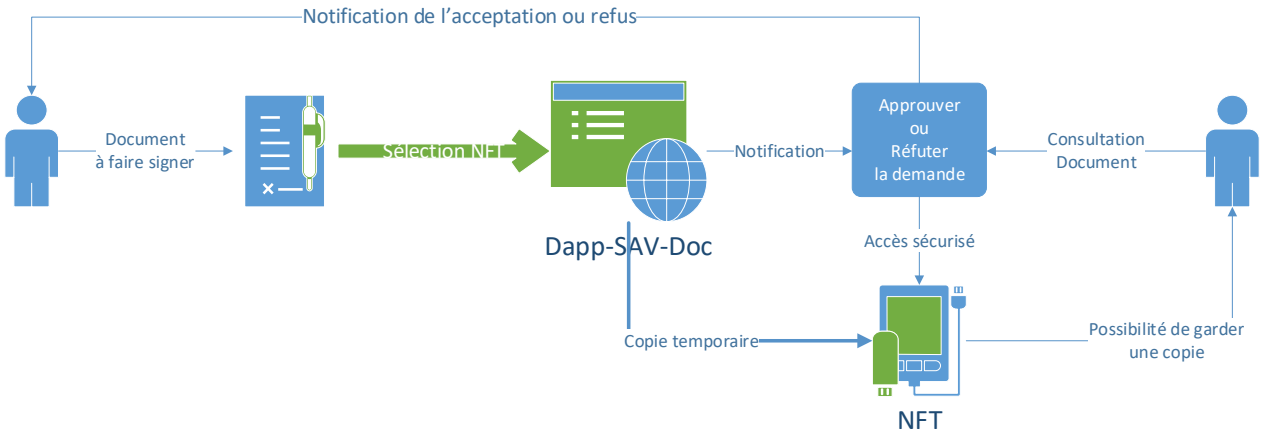
- Sauvegarder un Document



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



- Signer un document numériquement



Matrice de flux

Enregistrement sur l'application

Installation des composants nécessaires (métamask…) → validation demande inscription → création mot de passe maitre 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.

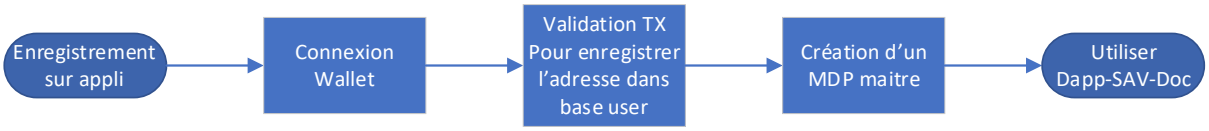
Demande de signature d'un document par un tiers → transmission d'une copie temporaire + notification au travers de l'appli au destinataire → possibilité de garder une copie → accepter ou non de signer

Vérification

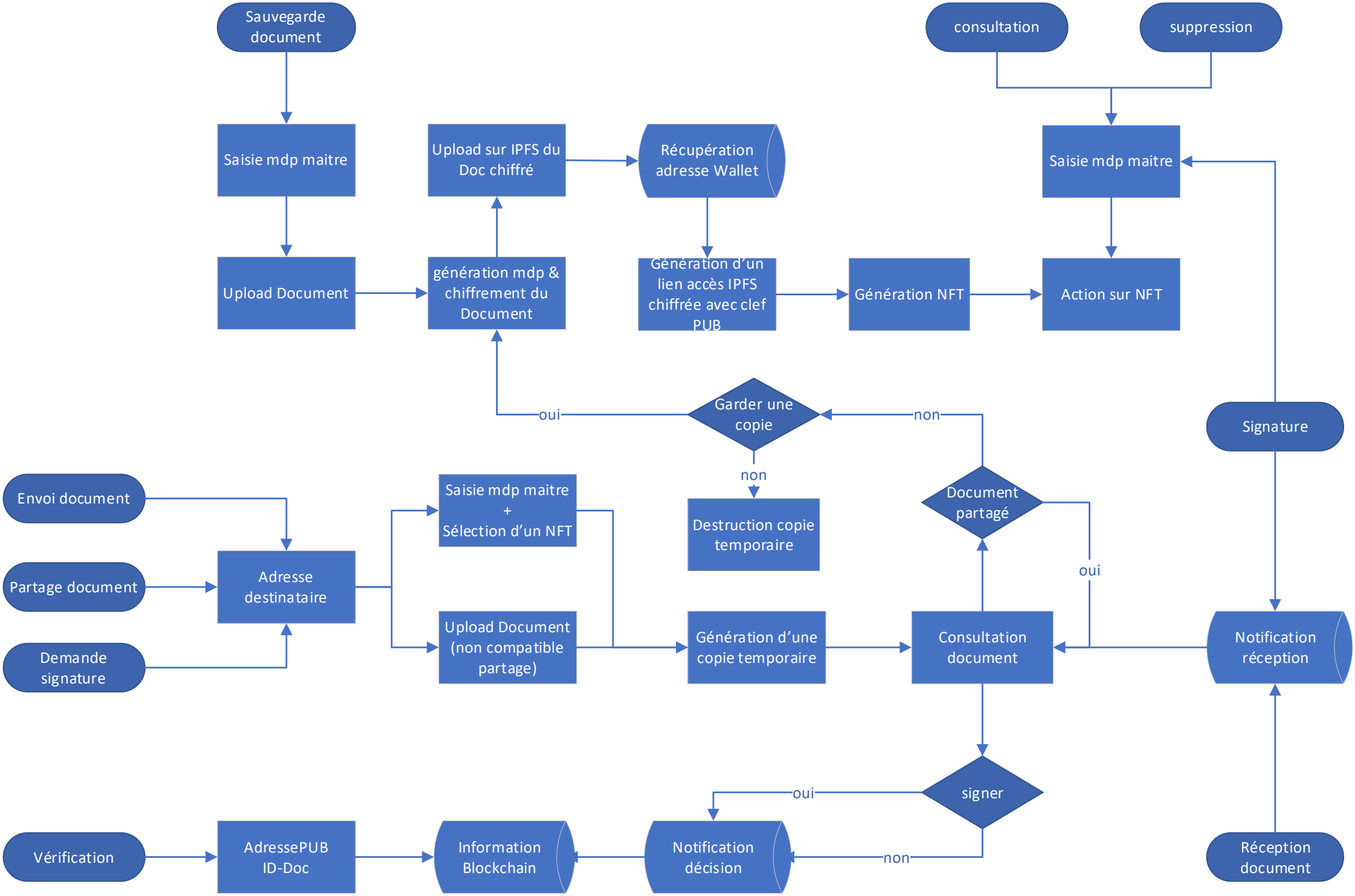
A partir de l'ID d'un document il est possible à n'importe qui de vérifier l'émetteur, les propriétaires et signataires.

Diagramme de Flux de SAV-Doc

Enregistrement



Utilisation


Sauvegarde document
Saisie mdp maitre
Upload Document
Upload sur IPFS du Doc chiffré
Récupération adresse Wallet
génération mdp & chiffrement du Document
Génération d'un lien accès IPFS chiffrée avec clef PUB
Génération NFT
consultation
suppression
Saisie mdp maitre
Action sur NFT
Garder une copie
oui
non
non
Signature
Envoi document
Partage document
Demande signature
Adresse destinataire
Saisie mdp maitre + Sélection d'un NFT
Upload Document (non compatible partage)
Destruction copie temporaire
Génération d'une copie temporaire
Document partagé
oui
Consultation document
Notification réception
signer
oui
non
Vérification
AdressePUB ID-Doc
Information Blockchain
Notification décision
Réception document

Explication du fonctionnement Technique

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 Ethreum est la Blockchain Turing complet disposant du plus haut niveau de décentralisation. Néanmoins son succès en fait également sa faiblesse de nombreuse Dapp se développent dessus mais son nombre de transaction journalière reste pour le moment bridée à 1,5Millions, ce qui amène en cas de sur-sollicitassions de cette dernière des frais de gas élevée.

Notre volume de transaction étant amené à devenir important sur notre application, le cout 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 cour 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 (différent 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 au 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 maitre. L'utilisateur n'a ainsi besoin que de retenir son mot de passe maitre et est assuré d'avoir un mot de passe solide pour chiffrer ses documents.

Stockage document : Pour stocker le document nous faisons appel à la technologie IPFS (system de stockage décentralisé en P2P). Les documents sont uploadés en étant chiffré 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 liens 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 associé 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 mdp maitre) 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 mdp maitre) 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 »

Répartition des fonctions

Front : Chiffrement du document ; upload IPFS

Mid : suppression IPFS

Back : Adresse des smart contract et détail de leur fonctionnalité

Expérience utilisateur

Le fonctionnement d'une blockchain et la manière d'interagir avec sont encore loin d'être rentrée dans les mœurs (risque majeur identifié à l'adoption de notre solution). Pour amoindrir cette problématique un ensemble de tuto sera à disposition pour accompagner l'utilisateur dans l'installation des composants nécessaires ainsi que lui vulgariser le fonctionnement de la Blockchain. Pour faire comprendre la notion de cout 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 l'ensemble des documents et signatures ainsi que leurs relations immuables dans le temps.

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 seront audités avant d'être déployé en production