



ROYAUME DU MAROC  
UNIVERSITE CHOUAIB DOUKKALI  
FACULTE DES SCIENCES EL JADIDA  
DEPARTEMENT D'INFORMATIQUE

جامعة شعيب الدكالي  
Université Chouaib Doukkali

# Projet de Fin d'étude

Pour l'obtention du Diplôme Licence Sciences Mathématiques  
et Informatiques

## Parcours Base de Données

Sous le thème

**Plateforme d'achat et de vente de documents numériques basée sur la Blockchain**

*Présenté par : BENNASSER EL MOSTAFA*

*Soutenu le 25 Juin 2025 devant les membres de jury :*

Pr. BOUTKHOUM OMAR	: Faculté des Sciences, El Jadida	Encadrant
Pr. SAADAOUI HASSAN	: Faculté des Sciences, El Jadida	Examinateur
Pr. ABADA DRISS	: Faculté des Sciences, El Jadida	Examinateur

Année universitaire 2024/2025

# Remerciements

Avant toute chose, je rends grâce à Allah, le Tout-Puissant, pour m'avoir accordé la force, la patience et la persévérence nécessaires pour mener à bien ce travail.

Je tiens à exprimer ma profonde gratitude Monsieur **BOUTKHOUM OMAR**, mon encadrant, pour sa disponibilité, ses conseils avisés, son accompagnement constant et la richesse de ses orientations tout au long de ce projet. Son expertise et son engagement ont grandement contribué à l'aboutissement de ce travail.

Mes sincères remerciements s'adressent également aux membres du **jury**, pour l'intérêt qu'ils ont porté à ce travail, le temps qu'ils lui ont consacré et les remarques constructives qu'ils ne manqueront pas d'apporter.

Je souhaite également remercier du fond du cœur **mes parents**, pour leur soutien moral et matériel tout au long de mes études, ainsi que **ma petite famille** et **mes amis**, pour leur présence, leurs encouragements et leur confiance tout au long de ce parcours académique.

---

# Résumé

Ce projet consiste à créer une application web permettant aux utilisateurs d'acheter et de vendre en toute sécurité des documents numériques tels que des articles universitaires, des guides et des modèles. Le système utilise la blockchain Ethereum pour gérer les transactions et les enregistrements de propriété, avec des contrats intelligents écrits en Solidity garantissant une gestion transparente et automatisée des achats, des rôles des utilisateurs et des listes de documents.

L'intégration de MetaMask permet aux utilisateurs de s'authentifier via leurs portefeuilles Ethereum, offrant ainsi une expérience de connexion et de paiement fluide. Les documents sont stockés sur IPFS sous forme chiffrée, et les acheteurs reçoivent la clé de déchiffrement après un achat, leur permettant d'accéder à leurs fichiers directement dans leur navigateur. Un système de notation et d'avis est également inclus, permettant aux acheteurs de laisser des commentaires stockés de manière immuable sur la blockchain.

L'interface de l'application a été conçue à l'aide de technologies web modernes, notamment React, Vite, TypeScript et Tailwind CSS, pour offrir une expérience utilisateur fluide et réactive. Le backend, développé avec Node.js, gère la vérification du portefeuille, la livraison sécurisée des clés et la gestion des sessions grâce à l'authentification JWT.

Ce projet démontre comment les technologies blockchain et Web peuvent être combinées pour créer des plateformes sécurisées et conviviales pour l'échange de contenu numérique.

Mots-clés : Blockchain Ethereum, Contrats intelligents, Solidity, MetaMask, IPFS, Chiffrement AES, React, Node.js, JWT, Application Web.

---

# Abstract

This project involves creating a web application that allows users to securely buy and sell digital documents such as academic articles, guides, and models. The system uses the Ethereum blockchain to manage transactions and ownership records, with smart contracts written in Solidity ensuring seamless and automated management of purchases, user roles, and document lists.

The MetaMask integration allows users to authenticate via their Ethereum wallets, providing a seamless login and payment experience. Documents are stored encrypted on IPFS, and buyers receive the decryption key after a purchase, allowing them to access their files directly in their browser. A rating and review system is also included, allowing buyers to leave comments stored immutably on the blockchain.

The application interface was designed using modern web technologies, including React, Vite, TypeScript, and Tailwind CSS, to provide a smooth and responsive user experience. The backend, developed with Node.js, handles wallet verification, secure key delivery, and session management using JWT authentication.

This project demonstrates how blockchain and web technologies can be combined to create secure and user-friendly platforms for exchanging digital content.

**Keywords:** Ethereum Blockchain, Smart Contracts, Solidity, MetaMask, IPFS, AES Encryption, React, Node.js, JWT, Web Application.

---

# Table des Matières

Chapitre 1 : .....	11
Contexte générale du Projet.....	11
1.1 Technologie Blockchain .....	12
1.2 Types de blockchain .....	13
1.3 Applications de la blockchain.....	14
1.4 Contrats intelligents .....	15
1.5 Énoncé du problème .....	16
1.6 Examen des solutions existantes.....	17
1.7 Objectif du projet.....	19
Chapitre 2 : .....	20
Étude préliminaire et fonctionnelle .....	20
2.1 Processus d'entreprise.....	21
2.1.1 Principe du chaînage de la blockchain .....	21
2.1.2 Coût des transactions en Ethereum.....	22
2.2 Étude préliminaire .....	22
2.3 Étude fonctionnelle .....	24
2.3.1 Spécifications fonctionnelles .....	24
2.3.2 Spécifications non fonctionnelles .....	25
2.4 Analyse de faisabilité du projet.....	26
2.4.1 Exigences générales.....	26

---

2.4.2 Contraintes attendues.....	27
2.4.3 Résultats attendus .....	31
Chapitre3 :.....	33
Analyse et conception.....	33
3.1 Langage de modélisation UML.....	34
3.2 Avantages d'UML .....	34
3.3 Conception et modélisation.....	35
3.3.1 Diagramme de cas d'utilisation.....	35
3.3.2 Diagrammes de séquence .....	36
3.3.2.1 Diagramme de séquence d'authentification .....	36
3.3.2.2 Diagramme de séquence de téléchargement.....	37
3.3.2.3 Diagramme de séquence d'achat.....	38
3.3.3 Diagramme de classes.....	39
Chapitre4 :.....	43
Choix Technique .....	43
4.1 Technologies et outils utilisés .....	44
4.1.1 Développement de la blockchain et des contrats intelligents .....	44
4.1.2 Backend .....	46
4.1.3 Interface utilisateur .....	47
4.1.4 Environnement de développement .....	48
4.2 ipfs .....	48
4.3 Mécanisme de chiffrement et de déchiffrement AES .....	49
4.4 Architecture Technique du Système.....	50
Chapitre 5 :.....	53
Réalisation .....	53
5.1 Mise en œuvre de l'application.....	54
5.1.1 Démonstration utilisateur.....	54

---

5.1.2 Démonstration administrateur .....	54
5.2 Phase de test .....	69
5.2.1 Tests .....	69
5.2.2 Limitations .....	70
Conclusion et perspectives .....	71
Bibliographie .....	73

---

# Liste des figures

FIGURE 1 TECHNOLOGIE BLOCKCHAIN .....	12
FIGURE 2 BLOCKCHAIN PUBLIQUE .....	13
FIGURE 3 BLOCKCHAIN PRIVEE.....	13
FIGURE 4 BLOCKCHAIN HYBRIDE .....	14
FIGURE 5 LE PROCESSUS D'UNE TRANSACTION DE CONTRAT INTELLIGENT .....	16
FIGURE 7 BLOCS DE CHAINAGE .....	21
FIGURE 10 DIAGRAMME DE CAS D'UTILISATION .....	36
FIGURE 11 DIAGRAMME DE SEQUENCE D'AUTHENTIFICATION .....	37
FIGURE 12 DIAGRAMME DE SEQUENCE DE TELECHARGEMENT .....	38
FIGURE 13 DIAGRAMME DE SEQUENCE D'ACHAT.....	39
FIGURE 14 DIAGRAMME DE CLASSES .....	41
FIGURE 15 ETHEREUM.....	44
FIGURE 16 SOLIDITY.....	44
FIGURE 17 HARDHAT .....	45
FIGURE 18 METAMASK.....	45
FIGURE 19 PIÑATA.....	46
FIGURE 20 NODE.JS .....	46
FIGURE 21 EXPRESS.JS.....	46
FIGURE 22 ETHERS.JS .....	47
FIGURE 23 REACT.JS .....	47
FIGURE 24 TAILWIND CSS.....	47
FIGURE 25 VS CODE .....	48
FIGURE 26 GIT .....	48
FIGURE 27 ARCHITECTURE TECHNIQUE .....	50
FIGURE 28 PAGE D'ACCUEIL 1 .....	55
FIGURE 29 PAGE D'ACCUEIL 2 .....	56
FIGURE 30 AUTHENTIFICATION.....	57
FIGURE 31 BIBLIOTHEQUE .....	59
FIGURE 32 DASHBOARD.....	60
FIGURE 33 ACHATS .....	60
FIGURE 34 DOCUMENTS TELEVERSES .....	61
FIGURE 35 HISTORIQUE DES VENTES .....	61
FIGURE 36 PAGE DE TELEVERSEMENT 1 .....	63
FIGURE 37 PAGE DE TELEVERSEMENT 2 .....	63
FIGURE 38 PAGE DE TELEVERSEMENT 3 .....	64
FIGURE 39 PAGE DE TELEVERSEMENT 4 .....	64
FIGURE 40 PAGE DE PROFIL 1 .....	65
FIGURE 41 PAGE DE PROFIL 2 .....	65
FIGURE 42 PAGE D'ADMIN 1 .....	66
FIGURE 43 PAGE D'ADMIN 2 .....	67
FIGURE 44 PAGE DOCUMENT 1.....	67
FIGURE 45 PAGE DOCUMENT 2.....	68

---

FIGURE 46 PAGE DOCUMENT 3 .....	68
FIGURE 47 CONFIRMATION DE TRANSACTION EFFECTUEE .....	69

## Liste des tableaux

TABLEAU 1 SOLUTIONS EXISTANTES .....	18
TABLEAU 2 CONTRAINTES TECHNOLOGIQUES.....	29
TABLEAU 3 CONTRAINTES ORGANISATIONNELLES .....	30

---

# Listes des abréviations

- **ETH** – Ethereum
- **IPFS** – Interplanetary File System
- **AES** – Advanced Encryption Standard
- **JWT** – JSON Web Token
- **NFT** – Non-Fungible Token
- **DAPP** – Decentralized Application
- **ENS** – Ethereum Name Service
- **EVM** – Ethereum Virtual Machine
- **JSON-RPC** – JavaScript Object Notation - Remote Procedure Call
- **OMG** – Object Management Group
- **SHA-256** – Secure Hash Algorithm 256-bit
- **SPA** – Single Page Application
- **Web3** – Web 3.0 (Decentralized Web)
- **MetaMask** – MetaMask (brand name)
- **Hardhat** – Hardhat (brand name)
- **Pinata** – Pinata (brand name)
- **React** – React (brand name)
- **Tailwind CSS** – Tailwind Cascading Style Sheets
- **Node.js** – Node.js (brand name)
- **Express.js** – Express.js (brand name)
- **Ethers.js** – Ethers.js (brand name)
- **Solidity** – Solidity (brand name)
- **TypeScript** – TypeScript (brand name)

---

# Introduction Générale

Les plateformes numériques traditionnelles sont confrontées à des défis majeurs pour garantir des transactions documentaires sécurisées, transparentes et inviolables. Leur architecture centralisée peut les exposer à des risques tels que l'accès non autorisé, la manipulation des données ou le manque de traçabilité des transactions. Face à la demande croissante de places de marché numériques fiables, il devient essentiel d'explorer des solutions plus robustes et décentralisées. Pour pallier ces limitations, ce projet intègre les fonctionnalités clés de la technologie blockchain, notamment l'immutabilité, la transparence et l'automatisation, afin de créer une place de marché sécurisée et orientée utilisateur pour les documents numériques. Dans ce système, les utilisateurs peuvent agir à la fois comme vendeurs et comme acheteurs, effectuant des transactions peer-to-peer entièrement automatisées grâce à des contrats intelligents. Chaque transaction est enregistrée de manière immuable sur la blockchain, garantissant ainsi l'équité et la traçabilité, et éliminant le recours aux intermédiaires. Les documents téléchargés sur la plateforme sont stockés de manière sécurisée grâce à IPFS ( InterPlanetary File System), un réseau de stockage décentralisé qui empêche la duplication non autorisée et garantit la disponibilité. Lorsqu'un acheteur achète un document, le fichier est chiffré grâce au chiffrement AES, et seul l'acheteur autorisé reçoit la clé de déchiffrement, préservant ainsi la confidentialité et contrôlant l'accès au contenu acheté. Ce rapport présente le développement d'une application web conçue pour gérer les ventes et l'accès aux documents numériques via la blockchain et le stockage décentralisé. Il commence par un aperçu des concepts pertinents tels que l'architecture blockchain, les contrats intelligents et IPFS. Il décrit ensuite le contexte du projet, les objectifs et l'approche de conception globale du système. De plus, les décisions techniques, les contraintes et les défis de mise en œuvre sont analysés en détail. Le rapport se conclut par une évaluation critique des résultats du projet, des suggestions d'améliorations futures et une réflexion sur les connaissances et compétences acquises tout au long du processus de développement.

---

# **Chapitre 1 :**

## **Contexte générale du Projet**

# Introduction

Le contexte général est un élément crucial de tout rapport de projet de fin d'études, car il fournit un cadre permettant de positionner le projet par rapport aux recherches et développements existants dans le domaine. Dans le contexte de la création d'une place de marché numérique sécurisée et transparente pour les documents grâce à la technologie blockchain, cette section est particulièrement importante. Elle met en évidence les différentes approches et solutions existantes visant à sécuriser les transactions, à protéger les contenus numériques et à permettre la traçabilité dans les environnements décentralisés.

## 1.1 Technologie Blockchain

La technologie blockchain est un enregistrement numérique décentralisé de transactions, partagé sur ONU réseau, immuable ou non. Elle permet de stocker, transmettre et mettre à jour des informations de toutes sortes de manière partagée entre plusieurs individus, fonctionnant en "peer-to-peer". Chaque participant a accès à une copie de la base de données et à tout l'historique qu'elle contient, avec une architecture décentralisée et une évolution autonome sans organe de contrôle central.

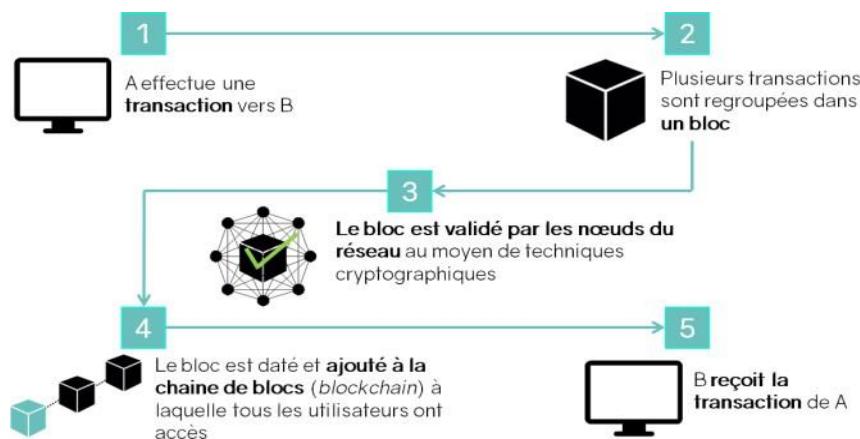


Figure 1 Technologie blockchain

## 1.2 Types de blockchain

### 1.2.1 Blockchain publique

Une blockchain publique est un système distribué accessible à tous, permettant à chacun de participer, de valider des transactions et d'assurer la sécurité du réseau. Cette technologie, ouverte à tous les utilisateurs, permet à chacun de rejoindre le réseau, de consulter des données ou d'effectuer des transactions. Elle fonctionne sans autorité centrale et se caractérise par une transparence absolue, un haut degré de décentralisation et une résistance à la censure. Principalement utilisées pour les cryptomonnaies (Bitcoin, Ethereum, Litecoin), les blockchains publiques protègent également les utilisateurs en prouvant que certaines opérations échappent au contrôle des développeurs d'applications.



Figure 2 Blockchain Publique

### 1.2.2 Blockchain privée

Une blockchain privée, également appelée blockchain autorisée, est un type de blockchain où certains priviléges sont réservés à des utilisateurs présélectionnés. Contrairement à une blockchain publique, une blockchain privée restreint l'accès et les actions aux participants autorisés, limitant la visibilité et la validation des informations à certains utilisateurs. Ce type de blockchain ne nécessite pas nécessairement l'utilisation d'une cryptomonnaie et peut offrir une sécurité renforcée à des entités telles que les grandes entreprises, les institutions financières et les organismes publics. Cependant, les blockchains privées peuvent présenter des inconvénients par rapport aux bases de données centralisées traditionnelles en termes de complexité, de gestion et de maintenance. Exemples : Hyperledger, Corda de R3, Quorum de JPMorgan.

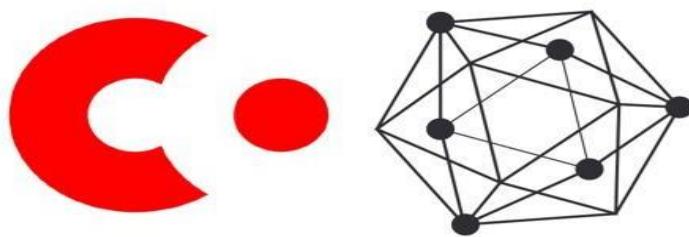


Figure 3 Blockchain privée

---

### 1.2.3 Blockchain de consortium (ou hybride)

La blockchain de consortium, également appelée blockchain hybride, est un modèle intermédiaire entre la blockchain publique et la blockchain privée. Elle est gérée par un groupe prédefini d'organisations qui contrôlent l'accès et la validation des transactions. La blockchain de consortium vise à combiner les avantages de la décentralisation avec un niveau de contrôle et de

Confidentialité plus élevée que les blockchains publiques traditionnelles. Ce modèle hybride s'avère pertinent pour de nombreuses applications nécessitant une gouvernance partagée entre plusieurs organisations.



Figure 4: Blockchain hybride

## 1.3 Applications de la blockchain

Les applications de la technologie blockchain sont diverses et impactent de nombreux secteurs. Elles incluent la gestion de la chaîne d'approvisionnement, l'identification numérique, le suivi des produits, la lutte contre la fraude bancaire, l'automatisation des assurances et l'investissement dans les stocks. Facilité d'échange, renforcement de la sécurité, et bien d'autres avantages. La blockchain offre des solutions innovantes pour améliorer la transparence, la sécurité et l'efficacité des processus dans divers secteurs, de la finance à la santé, en passant par l'immobilier et l'agroalimentaire. Voici quelques applications de la blockchain :

### 1.3.1 Transferts d'argent et paiements

La technologie blockchain a un impact significatif sur les transferts d'argent et les paiements internationaux. Elle rend ces transactions plus rapides, moins coûteuses et plus sécurisées. En effet, les blockchains permettent d'effectuer des transferts transfrontaliers quasi instantanément, réduisant ainsi le temps de traitement de plusieurs jours à quelques secondes.

De plus, l'utilisation de la blockchain pour les transferts d'argent permet de diminuer considérablement les frais de transaction, offrant des coûts plus transparents et réduits par rapport aux méthodes traditionnelles.

Cette technologie révolutionne le secteur du transfert d'argent en offrant des solutions plus efficaces, plus rapides et plus rentables, tout en améliorant la transparence et la sécurité des transactions financières internationales.

---

### **1.3.1 Échanges financiers**

La technologie blockchain est utilisée pour faciliter les transactions financières de diverses manières. Elle permet de créer des systèmes de règlement-livraison intégrés, offrant une traçabilité et une transparence accrues des échanges d'actifs. Les blockchains réduisent les coûts de transaction au sein des réseaux de paiement de détail des utilisateurs, offrant des solutions innovantes pour les paiements inter-clients, les échanges de cryptomonnaies, les services de transfert d'argent internationaux et les systèmes de paiement peer-to-peer. Les institutions financières commencent également à utiliser la blockchain pour développer des systèmes de paiement peer-to-peer, améliorant ainsi la liquidité et réduisant les besoins en garantie pour les échanges de titres les plus risqués. La blockchain révolutionne les échanges financiers en proposant des solutions décentralisées, transparentes, rapides et moins coûteuses que les services traditionnels.

### **1.3.2 Traçabilité des accès numériques via la blockchain**

La traçabilité des accès numériques est essentielle aux applications de la technologie blockchain. Elle permet l'enregistrement immuable et transparent de chaque interaction utilisateur avec une ressource numérique, comme une consultation, un téléchargement ou un transfert de droits d'accès. Grâce au registre distribué de la blockchain, chaque opération est horodatée, inviolable et accessible à tout moment pour vérification. Cela renforce la sécurité, la responsabilité et la transparence de la gestion des droits numériques, tout en réduisant les risques de fraude, de duplication ou d'accès non autorisé. Cette approche est particulièrement pertinente dans les environnements où le contrôle de l'accès et la protection des contenus sont essentiels.

## **1.4 Contrats intelligents**

Les contrats intelligents constituent une innovation majeure rendue possible par la technologie blockchain. Ils se définissent comme des programmes informatiques ou des protocoles de transaction conçus pour s'exécuter automatiquement lorsque des conditions prédéfinies sont remplies. L'objectif est de réduire le recours aux intermédiaires, les coûts d'arbitrage et les pertes dues à la fraude.

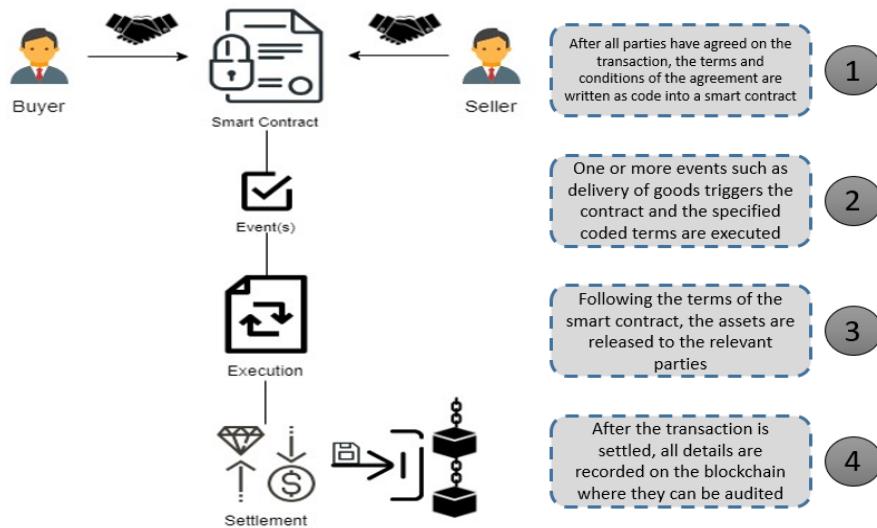


Figure 5 Le processus d'une transaction de contrat intelligent

Les contrats intelligents fonctionnent à l'aide d'instructions « si/quand... alors » codées en langage informatique. Lorsque les conditions sont remplies, le contrat s'exécute automatiquement sans intervention humaine. Les transactions sont enregistrées sur une blockchain, ce qui les rend sécurisées et immuables. Les contrats intelligents ont des applications nombreuses et variées, allant des transferts d'argent et des échanges financiers à la gestion de la chaîne d'approvisionnement, en passant par l'assurance, les élections, l'immobilier et la santé. Ils permettent l'automatisation des processus, la réduction des coûts et des erreurs, ainsi qu'une sécurité et une transparence accrues, le tout en supprimant le besoin d'intermédiaires. Cependant, les contrats intelligents ne sont pas sans défis. Ils soulèvent des questions de sécurité et d'intégrité des données, nécessitent l'harmonisation des parties prenantes et peuvent présenter une complexité de mise en œuvre et de gestion. Malgré ces défis, les contrats intelligents représentent une innovation majeure avec un potentiel d'application dans de nombreux secteurs.

## 1.5 Énoncé du problème

Les plateformes traditionnelles de distribution de documents numériques reposent sur des systèmes centralisés qui présentent des limites importantes en termes de confiance, de sécurité et de transparence. Le stockage centralisé des données crée un point de défaillance unique, rendant les plateformes vulnérables à la censure, à la suppression arbitraire de contenu ou à la perte d'accès due à des problèmes techniques ou à des décisions administratives.

---

Les utilisateurs ne disposent d'aucun moyen indépendant de vérifier l'intégrité ou l'historique des transactions, car ces systèmes manquent de traçabilité publique et d'enregistrements immuables. Ce manque de transparence favorise les manipulations et sape la confiance entre acheteurs et vendeurs. De plus, les paiements sont entièrement gérés par la plateforme elle-même, obligeant les utilisateurs à s'appuyer sur une autorité centrale pour l'exécution des transactions, sans aucune garantie décentralisée ni contrôle de la part de l'utilisateur.

Ces limitations entravent l'adoption de tels systèmes pour les documents précieux ou sensibles et exposent les utilisateurs à des fraudes potentielles, à des violations de données et à des pratiques déloyales.

## 1.6 Examen des solutions existantes

Avant de concevoir notre système, il est essentiel d'évaluer les solutions actuellement disponibles sur le marché. Cette analyse comparative nous permettra d'identifier leurs forces, leurs limites et les opportunités d'innovation offertes par notre approche combinant blockchain. Le tableau 1.2 présente une étude détaillée des principales plateformes de gestion de bibliothèque, mettant en évidence leurs fonctionnalités, les technologies utilisées et leurs faiblesses.

<b>Solution</b>	<b>Description</b>	<b>Avantages</b>	<b>Inconvénients</b>
<b>Livre . io</b>	Plateforme décentralisée de publication et d'échange de livres numériques utilisant Ethereum et IPFS. Permet aux créateurs de vendre des livres numériques avec un contrôle d'accès sécurisé via des contrats intelligents.	Interface conviviale, transactions sécurisées via blockchain, intégration avec IPFS, pas de frais de gaz pour les acheteurs, suivi de propriété.	Origines du projet académique, fonctionnalités limitées pour les marchés à grande échelle, dépendance à la configuration de portefeuilles tiers.
<b>OpenSea</b>	Place de marché basée sur la blockchain pour l'échange d'actifs numériques (par exemple, les NFT) sur Ethereum. Créateurs et acheteurs bénéficient d'un stockage décentralisé et d'une propriété basée sur des contrats intelligents.	Enregistrements de transactions évolutifs et immuables, adaptés au commerce de biens numériques, grande variété d'actifs pris en charge.	Complexité de déploiement, nécessite une infrastructure technique avancée, adoption limitée pour le trading de documents non NFT.
<b>Etsy</b>	Marché en ligne pour les produits artisanaux et numériques, avec des intégrations blockchain émergentes pour un suivi sécurisé de la provenance des articles numériques.	Transactions privées et sécurisées, éléments open source, contrôle granulaire des accès, base d'utilisateurs établie.	Déploiement complexe, nécessite une infrastructure pour l'adoption de la blockchain, adoption limitée de la blockchain dans le secteur.

Tableau 1 solutions existantes

---

## 1.7 Objectif du projet

La gestion et l'échange de documents numériques sont devenus de plus en plus importants dans le contexte du travail universitaire, professionnel et créatif. Cependant, les plateformes existantes manquent souvent de transparence, de vérifiabilité et de contrôle d'accès rigoureux, ce qui peut saper la confiance des utilisateurs et limiter le potentiel de transactions numériques équitables et sécurisées.

Grâce à notre projet, nous souhaitons créer une place de marché décentralisée permettant aux utilisateurs d'acheter et de vendre des documents numériques (PDF) dans un environnement sécurisé, transparent et contrôlé par l'utilisateur. Grâce aux contrats intelligents Ethereum, chaque transaction est enregistrée de manière immuable sur la blockchain, garantissant ainsi un suivi fiable de la propriété et de l'activité.

L'intégration du chiffrement AES et d'IPFS permet de stocker les documents de manière décentralisée tout en garantissant que seuls les utilisateurs autorisés peuvent accéder à leur contenu. Après un achat,

validé, l'acheteur reçoit une clé de décryptage qui lui permet de déverrouiller et de visualiser le fichier directement dans son navigateur, préservant ainsi la confidentialité et le contrôle.

LedgerDoc présente ainsi une solution moderne, évolutive et sécurisée qui répond au besoin croissant de plateformes de contenu numérique fiables, tout en favorisant l'autonomie des utilisateurs et en tirant parti des avantages des technologies décentralisées.

## Conclusion

Ce chapitre a posé les bases théoriques et technologiques du projet LedgerDoc en identifiant les faiblesses des plateformes de documents numériques traditionnelles, notamment leur manque de sécurité, de transparence et de contrôle par les utilisateurs. Il a démontré la pertinence d'une solution intégrant la blockchain et des technologies de stockage décentralisé pour garantir l'intégrité du système et un marché sécurisé et axé sur les utilisateurs. Après avoir validé la pertinence de cette approche, nous allons maintenant procéder à une analyse détaillée et aux choix de conception qui concrétiseront cette vision.

---

## Chapitre 2 :

# Étude préliminaire et fonctionnelle

# Introduction

Ce chapitre traite de l'étude fonctionnelle, phase cruciale de la conception d'un système d'information. Elle consiste en une analyse approfondie des besoins utilisateurs, visant à identifier les fonctionnalités requises par le système et à établir des spécifications fonctionnelles détaillées. Cette étape permet de s'assurer que LE système développé répondra efficacement aux besoins des utilisateurs finaux.

## 2.1 Processus d'entreprise

### 2.1.1 Principe du chaînage de la blockchain

La technologie blockchain facilite le stockage et la transmission sécurisés, transparents et immuables de données grâce à une séquence de blocs interconnectés, utilisant le hachage cryptographique. Dans ce contexte, chaque bloc encapsule plusieurs transactions, telles que les inscriptions d'utilisateurs, les téléchargements de documents, les achats et les avis, toutes enregistrées sur le réseau blockchain Ethereum.

Chaque fois qu'un utilisateur achète un document, ou télécharge du contenu, les données sont regroupées dans une transaction, hachées via SHA-256, puis intégrées dans un bloc lié cryptographiquement au précédent, garantissant un registre continu et sécurisé des activités de la plateforme.

L'adoption de ce principe de chaînage garantit que chaque interaction est enregistrée de manière permanente, traçable et inaltérable une fois validée par le réseau. Cette immuabilité, assurée par le mécanisme de consensus d'Ethereum, renforce l'intégrité des données et renforce la confiance entre les utilisateurs sur une place de marché décentralisée, conformément à l'objectif du projet : fournir un environnement sécurisé et fiable pour les échanges de documents.

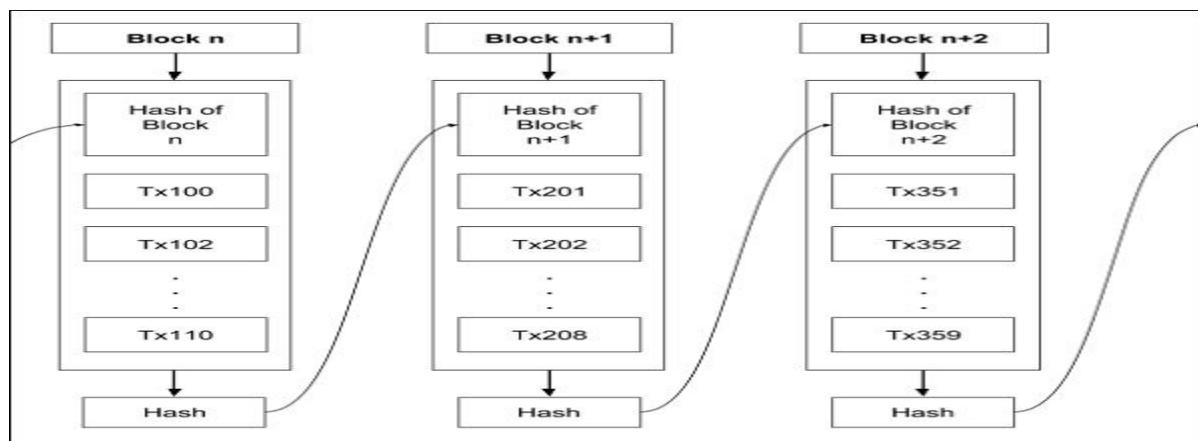


Figure 6 Blocs de chaînage

---

### **2.1.2 Coût des transactions en Ethereum**

Chaque action sur la plateforme, comme le téléchargement de contenu, l'achat d'un document ou la soumission d'un avis, implique l'exécution de fonctions de contrats intelligents sur la blockchain Ethereum. Ces exécutions nécessitent du « gaz », qui mesure l'effort de calcul nécessaire pour effectuer des transactions ou exécuter des contrats intelligents.

La consommation de gaz assure non seulement la sécurité, la traçabilité et l'immuabilité des données enregistrées, mais sert également à rémunérer les validateurs du réseau chargés du traitement des transactions.

Chaque fois qu'une transaction est effectuée, un montant approprié d'Ethereum (ETH) est dépensé pour couvrir les frais de transaction, garantissant que les opérations sont exécutées de manière fiable et sécurisée au sein de l'infrastructure décentralisée.

## **2.2 Étude préliminaire**

L'étude préliminaire constitue une phase fondamentale de la planification de notre plateforme de partage de documents basée sur la blockchain. Elle permet d'évaluer la faisabilité technique, de définir les exigences fonctionnelles essentielles, de choisir les technologies appropriées et d'anticiper les défis liés à l'intégration des contrats intelligents Ethereum, du stockage décentralisé via IPFS et d'un assistant chatbot IA simple.

Cette phase garantit également que le périmètre du projet est bien défini et aligné sur les priorités de développement. Elle nous permet de nous concentrer sur les fonctionnalités les plus critiques tout en concevant un système évolutif.

Notre plateforme distingue deux principaux rôles d'utilisateur : l'**Utilisateur (Acheteur/Vendeur)** et l'**Administrateur**.

#### **• Utilisateur (acheteur/vendeur)**

Les utilisateurs sont les principaux acteurs de la plateforme. Ils s'authentifient via un compte standard ou une connexion décentralisée via un portefeuille Ethereum (par exemple, MetaMask). Une fois connectés, ils peuvent :

#### **Parcourir et explorer les documents :**

les utilisateurs peuvent parcourir la plateforme par catégorie de document, auteur, titre ou mots-clés. Chaque fiche inclut des métadonnées détaillées, le prix, un aperçu et les conditions d'accès.

- 
- **Documents d'achat :**  
lorsqu'un utilisateur achète un document, un contrat intelligent enregistre la transaction sur la blockchain Ethereum. L'utilisateur reçoit les droits d'accès et le fichier chiffré est livré en toute sécurité via IPFS. Seul l'acheteur peut le déchiffrer à l'aide de la clé AES fournie.
  - **Gestion des activités personnelles :**  
les utilisateurs peuvent consulter leur historique d'achats et accéder à nouveau aux documents précédemment acquis. Chaque action est enregistrée de manière transparente et immuable sur la chaîne.
  - **Obtenez de l'aide via Chatbot**  
Un assistant chatbot léger et alimenté par l'IA est disponible pour guider les utilisateurs tout au long du processus.  
plateforme répondant aux questions liées à la navigation, aux achats, à la connexion au portefeuille, etc.
- **Administrateur**
- L'administrateur supervise la modération et le contrôle du système de la plateforme. Grâce à une interface d'administration sécurisée, il peut :
- **Gérer les utilisateurs**  
Affichez une liste de tous les utilisateurs et activez ou suspendez les comptes en cas de violations ou d'inactivité.
  - **Modération du contenu**  
Accédez aux documents téléchargés et gérez-les. L'administrateur peut supprimer tout contenu non conforme aux règles de la plateforme ou sur demande.

Cette répartition claire des responsabilités garantit un fonctionnement fluide, une transparence et un contrôle décentralisé du partage de documents, tout en tirant parti des technologies Ethereum et IPFS pour la sécurité, la traçabilité et l'équité.

---

## 2.3 Étude fonctionnelle

L'étude fonctionnelle est une étape fondamentale du développement de notre projet. Elle consiste à analyser les besoins des utilisateurs, à concevoir la structure du système, à documenter les spécifications détaillées, à valider les solutions proposées et à piloter le développement ultérieur.

### 2.3.1 Spécifications fonctionnelles

#### Fonctionnalités utilisateur (acheteur/vendeur)

Les utilisateurs jouent le double rôle d'acheteur et/ou de vendeur, avec accès aux fonctionnalités suivantes :

- **Parcourir et rechercher des documents** : Explorez le catalogue par titre, catégorie ou mot-clé. Chaque document présente un aperçu, un prix et des métadonnées.
- **Documents d'achat** : Lors de l'achat d'un document, un contrat intelligent gère la transaction. L'utilisateur reçoit les droits d'accès et la clé de déchiffrement du fichier chiffré stocké sur IPFS.
- **Téléchargement de documents** : Les utilisateurs peuvent télécharger des documents PDF destinés à la vente. Les métadonnées (titre, description, prix) sont fournies, et le document est chiffré et stocké sur IPFS. Le téléchargement est enregistré en chaîne via des contrats intelligents.
- **Suivre l'activité personnelle** : afficher l'historique personnel, y compris les documents téléchargés et achetés.
- **Assistance Chatbot** : un assistant alimenté par l'IA aide les utilisateurs à naviguer, à se connecter au portefeuille et à les guider dans leur utilisation.

#### Fonctionnalités de l'administrateur

L'administrateur est responsable de la modération et du contrôle opérationnel de la plateforme. Grâce à une interface sécurisée, il peut :

- **Gestion des utilisateurs** : affichez, suspendez ou réactivez les comptes utilisateurs en cas de violation des politiques ou d'inactivité.
- **Gestion de contenu** : Accédez à tous les documents téléchargés. L'administrateur peut supprimer tout document qui enfreint les conditions d'utilisation ou sur demande.

---

### 2.3.2 Spécifications non fonctionnelles

Pour garantir un fonctionnement efficace, sécurisé et fiable, les exigences non fonctionnelles suivantes définissent les attributs de qualité clés attendus de notre plateforme de partage de documents :

- **Performances** : La plateforme doit gérer un volume élevé de téléchargements de documents, d'achats et d'interactions avec les chatbots simultanés avec un temps de réponse court. Les opérations clés, telles que la connexion au portefeuille, l'accès aux fichiers chiffrés et la récupération des métadonnées, doivent rester réactives même en période de forte utilisation.
- **Sécurité** : Le système assure une protection robuste des opérations sensibles et des données utilisateur. Les documents téléchargés sont chiffrés en arrière-plan avant d'être stockés sur IPFS. Le déchiffrement est effectué en front-end à l'aide de clés AES, accessibles uniquement aux utilisateurs autorisés après un achat réussi. Toutes les transactions, telles que les achats et les téléchargements, sont enregistrées de manière immuable sur la blockchain Ethereum via des contrats intelligents.
- **Évolutivité** : La plateforme est conçue pour évoluer au rythme des besoins des utilisateurs. Son architecture répartit les problématiques liées au stockage décentralisé (IPFS), à la logique blockchain (contrats intelligents Ethereum) et aux services back-end centralisés (par exemple, chiffrement, assistant de chat). Cette structure en couches permet une évolutivité horizontale des services tels que le traitement des documents, la gestion des métadonnées et l'assistance IA, sans compromettre les performances du système.
- **Fiabilité** : Les mécanismes de contrats intelligents garantissent un traitement déterministe et traçable des actions clés des utilisateurs. Qu'il s'agisse d'accéder à un document acheté ou d'en télécharger un nouveau, le système doit se comporter de manière cohérente et se remettre en marche sans problème après une panne. Les utilisateurs doivent toujours pouvoir récupérer en toute sécurité le contenu précédemment acheté.
- **Portabilité** : La plateforme doit fonctionner correctement sur tous les navigateurs modernes (Chrome, Firefox, Edge) et les principaux systèmes d'exploitation (Windows, macOS, Linux). En tant qu'application décentralisée web, elle est intrinsèquement portable et ne nécessite aucune installation ni configuration spécifique au système d'exploitation.
- **Ergonomie** : L'interface utilisateur doit être simple, claire et facile à parcourir. Des fonctionnalités telles que l'authentification par portefeuille, l'aperçu des documents et l'assistant chatbot doivent offrir une expérience utilisateur fluide, même pour les utilisateurs moins technologiques.

---

utilisateurs non techniques. La plateforme minimise la charge cognitive tout en préservant l'intégralité des fonctionnalités.

- **Conformité** : La plateforme doit se conformer aux réglementations applicables en matière de confidentialité des données et de protection des utilisateurs. Les enregistrements publics de la blockchain contribuent à garantir la transparence, tandis que les fichiers chiffrés hébergés sur IPFS empêchent la diffusion non autorisée de contenu payant.
- **Maintenabilité** : Le système doit respecter les principes de conception modulaire et être bien documenté afin de faciliter le développement, le débogage et les mises à niveau futurs. Chaque composant majeur (contrats intelligents, chiffrement backend, interaction IPFS, interface utilisateur frontend) est isolé et testable indépendamment.

## 2.4 Analyse de faisabilité du projet

Dans un premier temps, nous avons mené une étude de faisabilité approfondie de notre plateforme de partage de documents. Cette phase visait à évaluer les exigences fonctionnelles et les contraintes techniques liées à l'intégration de la technologie blockchain, notamment IPFS pour le stockage décentralisé.

Cela nous a également permis d'évaluer les avantages potentiels de cette solution pour les plateformes de distribution de contenu numérique. Il était crucial de comprendre tous les aspects de ce système innovant, notamment son architecture technique et les défis prévisibles de sa mise en œuvre. Identifier clairement ces facteurs dès le départ nous a permis de construire une base solide pour un développement structuré et une exécution réussie du projet.

### 2.4.1 Exigences générales

Avant d'atteindre les principaux objectifs de notre plateforme de partage de documents, il est essentiel de définir les exigences fondamentales attendues du système. Ces exigences permettent de définir clairement les fonctionnalités à implémenter pour répondre aux besoins spécifiques des créateurs, acheteurs et administrateurs de documents au sein de l'écosystème.

L'identification de ces exigences majeures dès le départ permet d'établir une feuille de route solide, garantissant la pertinence, la convivialité et l'intégrité fonctionnelle tout au long du développement de la plateforme.

- 
- **Interfaces basées sur les rôles** : chaque type d'utilisateur (acheteur, vendeur ou administrateur) dispose d'une interface dédiée adaptée à ses actions et droits d'accès spécifiques.
  - **Authentification par portefeuille** : les utilisateurs se connectent à la plateforme via leur portefeuille Ethereum (par exemple, MetaMask). Cela garantit une vérification d'identité sécurisée et décentralisée, sans nécessiter de connexion traditionnelle par nom d'utilisateur et mot de passe.

**Gestion du catalogue de documents** : Tous les utilisateurs peuvent parcourir et effectuer des recherches dans un catalogue complet de documents. Chaque document comprend des métadonnées telles que le titre, la description, le prix, l'aperçu et le statut IPFS.

**Système d'achat sécurisé et de traçabilité** : Les achats sont gérés via des contrats intelligents Ethereum, garantissant un suivi immuable et transparent des transactions. Les documents sont chiffrés et stockés sur IPFS, avec un accès contrôlé par des clés de déchiffrement délivrées après l'achat.

**Protection des données** : Le système garantit que les informations personnelles des utilisateurs, les documents cryptés et l'historique des achats sont protégés contre tout accès non autorisé, conformément aux normes modernes de protection des données.

**Compatibilité entre navigateurs** : la plate-forme prend en charge tous les principaux navigateurs Web (par exemple, Chrome, Firefox, Edge), garantissant une expérience utilisateur cohérente et accessible sur différents systèmes.

**Assistant chatbot IA léger** : Bien qu'il ne s'agisse pas d'un système de recommandation complet, le chatbot intégré aide les utilisateurs à naviguer sur la plateforme, à résoudre les problèmes, à connecter leurs portefeuilles et à comprendre comment acheter ou télécharger des documents. Il favorise un meilleur engagement et simplifie les interactions avec les nouveaux utilisateurs.

**Maintenance et support continu** : La plateforme est conçue dans un souci de maintenance à long terme, incluant une architecture modulaire, des mises à jour régulières et un support technique pour garantir la fiabilité et répondre aux besoins évolutifs des utilisateurs.

#### 2.4.2 Contraintes attendues

Tout projet innovant impliquant des technologies émergentes est confronté à des défis et des menaces lors de sa mise en œuvre. C'est pourquoi il est crucial de documenter soigneusement toutes les contraintes à prendre en compte tout au long du processus avant de procéder au déploiement.

Cette approche proactive nous permettra d'anticiper et de surmonter efficacement les obstacles potentiels, assurant ainsi le succès et la viabilité à long terme du projet.

Les tableaux suivants 1 et 2 , détaille l'ensemble des contraintes techniques et organisationnelles qui peuvent survenir lors du développement de notre plateforme et de l'affinement de notre projet.

Contraintes technologiques		
Contraintes	Problème	Impact
<b>Évolutivité de réseau</b>	Ethereum, bien que plus efficace depuis le passage au Proof-of-Stake, maintient une limite fondamentale d'environ 30 transactions par seconde (contre des milliers pour les systèmes bancaires traditionnels). Ce limitation Est inhérent a son architecture décentralisée.	En période de forte activité (par exemple, en cas d'achats ou de téléchargements simultanés de nombreux documents), les utilisateurs peuvent être confrontés à des retards dans la confirmation des transactions. Cela peut entraîner une mauvaise expérience utilisateur (en particulier pour les achats ou téléchargements urgents), décourager l'utilisation de la plateforme ou inciter les utilisateurs à l'abandonner.
<b>Frais de transaction</b>	Les frais de gaz (le coût d'exécution d'une transaction) varient en fonction de la congestion du réseau, parfois de manière imprévisible.	Si de nombreux utilisateurs achètent ou téléchargent des documents simultanément, les frais de transaction peuvent grimper, rendant difficile toute prévision des coûts pour les utilisateurs ou la plateforme. Cette imprévisibilité peut dissuader les utilisateurs de télécharger du contenu ou de finaliser des achats, surtout si les frais sont supérieurs au prix du document.

<b>Complexité de la contrats intelligents</b>	Une fois déployés, les contrats intelligents sont immuables. Toute erreur de code (même mineure) ne peut être corrigé sans déployer de nouveau contrat. La rédaction de contrats sécurisés nécessite une compétence très avancée dans les modèles de solidité et de sécurité blockchain.	Une vulnérabilité dans votre contrat (par exemple, lors du téléchargement ou de l'achat d'un document...) pourrait compromettre l'accès aux documents, permettre des abus (par exemple, des téléchargements non autorisés) ou bloquer définitivement l'accès aux fichiers achetés. La correction de ce problème nécessiterait un redéploiement et une nouvelle migration des utilisateurs, avec un risque de perte de confiance.
<b>Intégration avec les systèmes hors chaîne</b>	La plateforme repose sur des composants hors chaîne tels que le serveur back-end (pour le chiffrement, l'authentification et la gestion des clés) et IPFS (pour le stockage décentralisé des fichiers). Ces systèmes ne sont pas intrinsèquement vérifiables par la blockchain.	Après un achat on-chain réussi, l'acheteur s'attend à accéder au fichier chiffré correspondant et à recevoir la clé de déchiffrement. En cas de défaillance, de compromission ou d'indisponibilité du backend, l'utilisateur risque de perdre l'accès au contenu acheté malgré la transaction on-chain, ce qui peut entraîner une perte de confiance et un mécontentement de la part de l'utilisateur.

Tableau 2 Contraintes technologiques

Contraintes organisationnelles		
Contraintes	Problème	Impact
<b>Adoption par le personnel</b>	Passer d'un système traditionnel à une plateforme de partage de documents basée sur la blockchain nécessite une transformation significative des flux de travail. Les administrateurs et les modérateurs doivent maîtriser la gestion des portefeuilles, l'interaction avec les contrats intelligents et la sécurisation des opérations back-end.	La résistance au changement peut entraîner des retards d'intégration. La productivité pourrait chuter temporairement pendant que les administrateurs s'adaptent au nouveau système. Des malentendus concernant la gestion des portefeuilles ou les autorisations contractuelles peuvent entraîner des erreurs opérationnelles ou des problèmes de modération de contenu, perturbant ainsi l'expérience utilisateur.
<b>Intégration avec les sources de documents traditionnelles</b>	Tous les documents ou éditeurs ne prennent pas en charge la distribution basée sur la blockchain, le chiffrement ou l'hébergement décentralisé de fichiers. Des problèmes juridiques, de licence ou de compatibilité de format peuvent survenir pour les fichiers existants ou les contributions institutionnelles.	Cela peut nécessiter le maintien d'un système parallèle hors chaîne pour le contenu plus ancien ou incompatible, augmentant la complexité de la gestion de la plateforme et potentiellement déroutant pour les utilisateurs quant à la disponibilité des documents ou aux mécanismes d'accès.
<b>Gestion de la identités numériques</b>	La nécessité pour les utilisateurs de gérer leurs portefeuilles de cryptomonnaies et leurs clés privées peut constituer un obstacle majeur, en particulier pour ceux qui ne sont pas familiarisés avec les technologies blockchain. Il n'existe pas de mécanisme de « mot de passe oublié » pour les portefeuilles.	Jusqu'à 40 à 60 % des utilisateurs (notamment les seniors, les étudiants peu familiarisés avec le Web3 ou les personnes ayant un accès limité aux outils numériques) peuvent rencontrer des difficultés d'accès à la plateforme. Cela peut impacter son adoption et réduire son inclusivité, limitant ainsi sa portée et son utilité auprès de divers groupes d'utilisateurs.

Tableau 3 Contraintes organisationnelles

---

Les tableaux précédents ont mis en évidence les principaux défis techniques et organisationnels de notre plateforme, notamment la complexité de l'intégration de la technologie blockchain , la protection des données sensibles des utilisateurs et les difficultés liées à l'adoption par les utilisateurs et à l'interopérabilité avec les systèmes existants. Identifier et traiter ces contraintes dès la phase de conception est essentiel pour garantir un déploiement réussi et la satisfaction durable de toutes les parties prenantes.

#### **2.4.3 Résultats attendus**

Notre plateforme de marché de documents intelligents, intégrant les technologies en chaîne et hors chaîne, apportera les améliorations majeures suivantes :

**Efficacité opérationnelle accrue** : les contrats intelligents automatisent les achats de documents et les droits d'accès, réduisant les opérations manuelles de plus de 70 % et permettant des transactions quasi instantanées en quelques secondes.

**Transparence et traçabilité** : La blockchain fournit un historique immuable de toutes les transactions de documents (téléchargements, achats, décryptages), garantissant une traçabilité et une responsabilité complètes.

**Disponibilité instantanée** : le statut du document (disponible, acheté, supprimé) est mis à jour instantanément dans l'ensemble du système, éliminant ainsi les retards de synchronisation souvent rencontrés dans les systèmes traditionnels.

**Sécurité et confidentialité** : L'authentification par portefeuille et le chiffrement AES garantissent que seuls les utilisateurs autorisés, tels que les acheteurs ou les personnes ayant téléchargé des documents, peuvent déchiffrer et accéder au contenu acheté. Les contrats intelligents blockchain gèrent le contrôle d'accès et enregistrent l'historique immuable de propriété et de transactions.

**Expérience utilisateur améliorée** : La plateforme n'exige pas de données personnelles des utilisateurs. Ils s'authentifient uniquement via l'adresse de leur portefeuille. Les champs facultatifs tels que le nom et l'adresse e-mail ne sont pas obligatoires. Seules les données blockchain pseudonymes (par exemple, l'adresse du portefeuille et les métadonnées de transaction) sont enregistrées, garantissant ainsi une confidentialité et une conformité optimales dès la conception.

**Évolutivité** : La structure modulaire du système permet des mises à jour transparentes et l'intégration de nouvelles fonctionnalités sans perturber les services existants.

En résumé, notre marché de documents alimenté par la blockchain et l'IA modernisera la distribution de contenu numérique en automatisant les transactions, en sécurisant les données

---

sensibles, en garantissant une traçabilité complète et en améliorant l'expérience utilisateur globale, tout en restant conforme aux normes juridiques applicables.

## Conclusion

En conclusion, cette phase préparatoire a permis de définir clairement les exigences fonctionnelles et techniques de la plateforme, tout en évaluant sa faisabilité grâce à l'étude des technologies sélectionnées. Les défis identifiés, notamment en termes de sécurité, d'évolutivité et de complexité technique, ont été anticipés afin de guider efficacement les prochaines étapes du projet. Nous allons maintenant entamer la phase d'analyse et de conception, étape clé au cours de laquelle ces exigences seront traduites en modèles concrets et en une architecture technique détaillée, posant ainsi les bases du développement à venir.

---

# **Chapitre3 :**

## Analyse et conception

---

# Introduction

Dans ce chapitre, nous explorerons en détail les différents diagrammes UML que nous avons développés pour notre projet, notamment des diagrammes de cas d'utilisation, des diagrammes de séquence et des diagrammes de classes. Nous présenterons également l'architecture de notre projet en décrivant les principaux composants, leurs interactions et les technologies utilisées pour les implémenter.

## 3.1 Langage de modélisation UML

**UML (Unified Modeling Language)** est un langage graphique de modélisation informatique. Ce langage est aujourd'hui la référence en modélisation objet, ou programmation orientée objet. Cette dernière consiste à modéliser des éléments du monde réel sous la forme d'un ensemble d'entités informatiques appelées « objets ».

UML se compose de diagrammes permettant de visualiser et de décrire la structure et le comportement des objets d'un système. Il permet de présenter des systèmes logiciels complexes de manière plus simple et plus compréhensible qu'avec du code informatique. **UML** trouve des applications dans le développement logiciel, mais aussi dans l'industrie (pour la modélisation des flux de processus, par exemple), en ingénierie et en marketing.

UML 1.0 a été adopté comme norme par l'Object Management Group (OMG) en janvier 1997. Il est issu de la fusion de trois méthodes orientées objet développées par Grady Booch, Jim Rumbaugh et Ivar Jacobson. Les versions successives ont depuis été validées.

## 3.2 Avantages d'UML

Dans le cadre d'un projet informatique de système d'information (SI), l'utilisation de la modélisation UML apporte de nombreux avantages qui impactent

- Modularité
- Abstraction
- Encapsulation

Structuration cohérente des fonctionnalités et des données

Cela permet également, à un stade précoce, de définir clairement les besoins du client, évitant ainsi les dépassements de coûts liés à la livraison d'un logiciel qui ne satisfait pas le client.

---

De plus, la modélisation UML simplifie les aspects liés à la conception et à l'architecture du logiciel pour le client. Elle permet également une compréhension rapide du programme par d'autres développeurs externes en cas de transfert du logiciel et facilite sa maintenance.

### **3.3 Conception et modélisation**

La conception désigne la phase du processus de développement au cours de laquelle les spécifications et les plans détaillés sont élaborés pour la mise en œuvre d'un projet. Cela implique la création d'architectures logicielles, de schémas de bases de données, de modèles de données et d'interfaces utilisateur.

L'objectif de la conception est de traduire les exigences fonctionnelles et non fonctionnelles identifiées lors de la phase d'analyse en une solution technique viable et réalisable. Elle prend en compte des considérations telles que l'évolutivité, la sécurité, la maintenabilité et l'efficacité opérationnelle du système.

De plus, la phase de conception peut impliquer des itérations et des ajustements en fonction des commentaires des parties prenantes et des contraintes du projet.

#### **3.3.1 Diagramme de cas d'utilisation**

Le diagramme des cas d'utilisation figure 10 présente les fonctionnalités clés de notre plateforme de gestion de documents basée sur la blockchain. Deux acteurs principaux sont identifiés :

##### **1. Utilisateur**

Après s'être authentifié avec MetaMask, l'utilisateur peut :

- Parcourir les documents disponibles.
- Rechercher des documents spécifiques.
- Achetez des documents en utilisant ETH.
- Télécharger les documents achetés (décryptés côté client).
- Laissez les notes (stockées sur la chaîne).

L'intégration de la blockchain garantit des transactions transparentes et sécurisées.

##### **2. Administrateur**

L'administrateur a des privilèges élevés pour :

- Suspendre/activer les comptes utilisateurs.
- Supprimez les documents inappropriés.

- Afficher les listes d'utilisateurs et de documents.

Toutes les actions nécessitent une authentification.

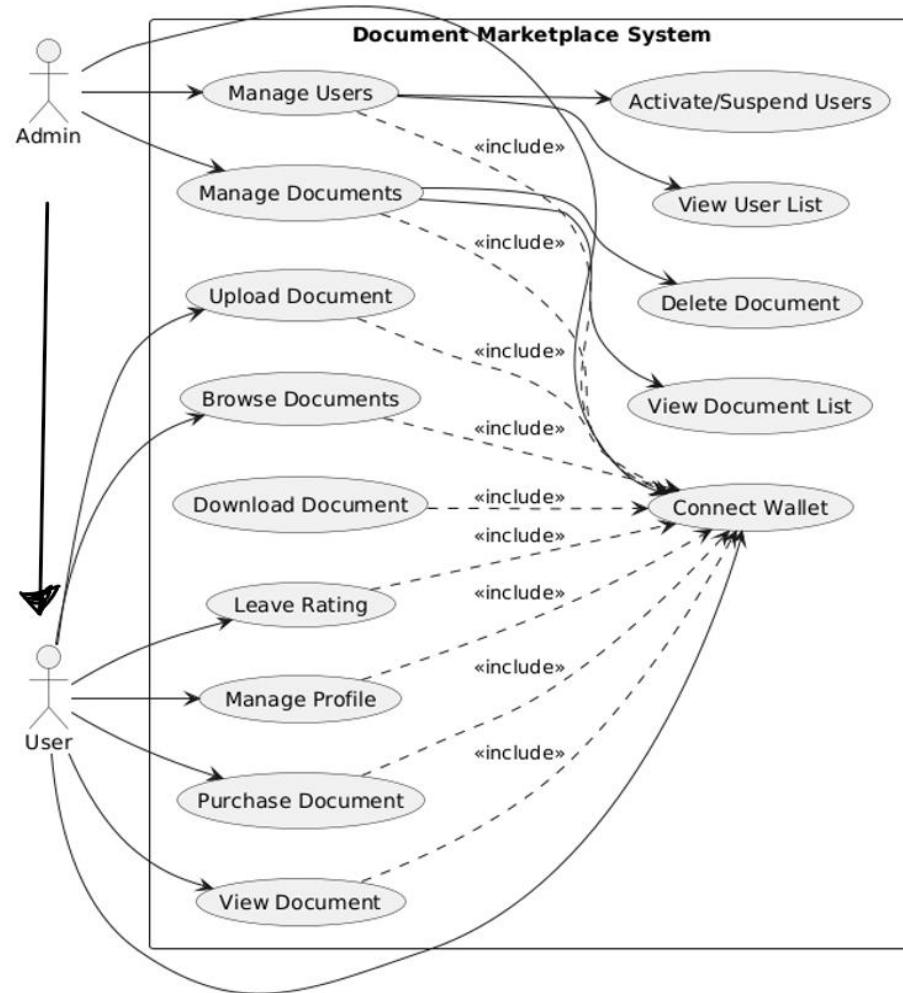


Figure 7 Diagramme de cas d'utilisation

### 3.3.2 Diagrammes de séquence

#### 3.3.2.1 Diagramme de séquence d'authentification

Le diagramme de séquence de la figure 11 illustre le processus d'authentification complet de la plateforme. Il détaille trois scénarios clés : la connexion au portefeuille, la vérification d'identité et l'enregistrement automatique de l'utilisateur sur la blockchain. Lors de la connexion, l'utilisateur clique sur un bouton dédié pour connecter son portefeuille via MetaMask, ce qui déclenche une demande de signature d'un message d'authentification à durée déterminée. Ce

message signé est ensuite envoyé au backend, qui vérifie l'identité de l'utilisateur en récupérant l'adresse du portefeuille. Si l'adresse est déjà enregistrée dans le contrat intelligent, un jeton JWT est émis pour établir une session sécurisée. Sinon, l'utilisateur est automatiquement enregistré sur la blockchain avant de recevoir le jeton JWT. Chaque étape implique différents acteurs techniques, notamment l'interface utilisateur, le portefeuille MetaMask, le serveur backend et le contrat intelligent, afin de garantir un flux d'authentification fluide et sécurisé, tout en préservant la transparence et la traçabilité grâce à l'intégration à la blockchain.

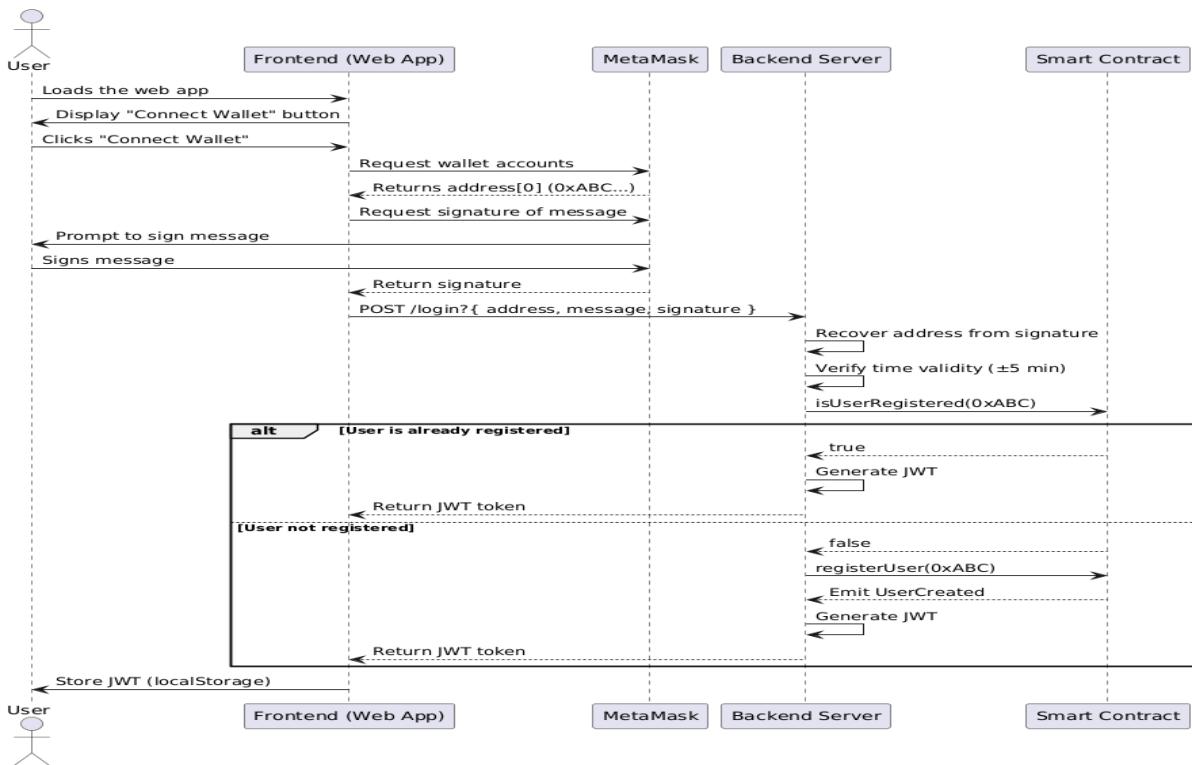


Figure 8 Diagramme de séquence d'authentification

### 3.3.2.2 Diagramme de séquence de téléchargement

Le diagramme de séquence de la figure 12 décrit le processus de téléchargement d'un document après authentification de l'utilisateur. Une fois le formulaire de téléchargement rempli, le backend vérifie le JWT, génère un aperçu, chiffre le fichier, télécharge les données sur IPFS, stocke la clé AES et enregistre le document sur la blockchain. Le document est ensuite mis à disposition sur la plateforme.

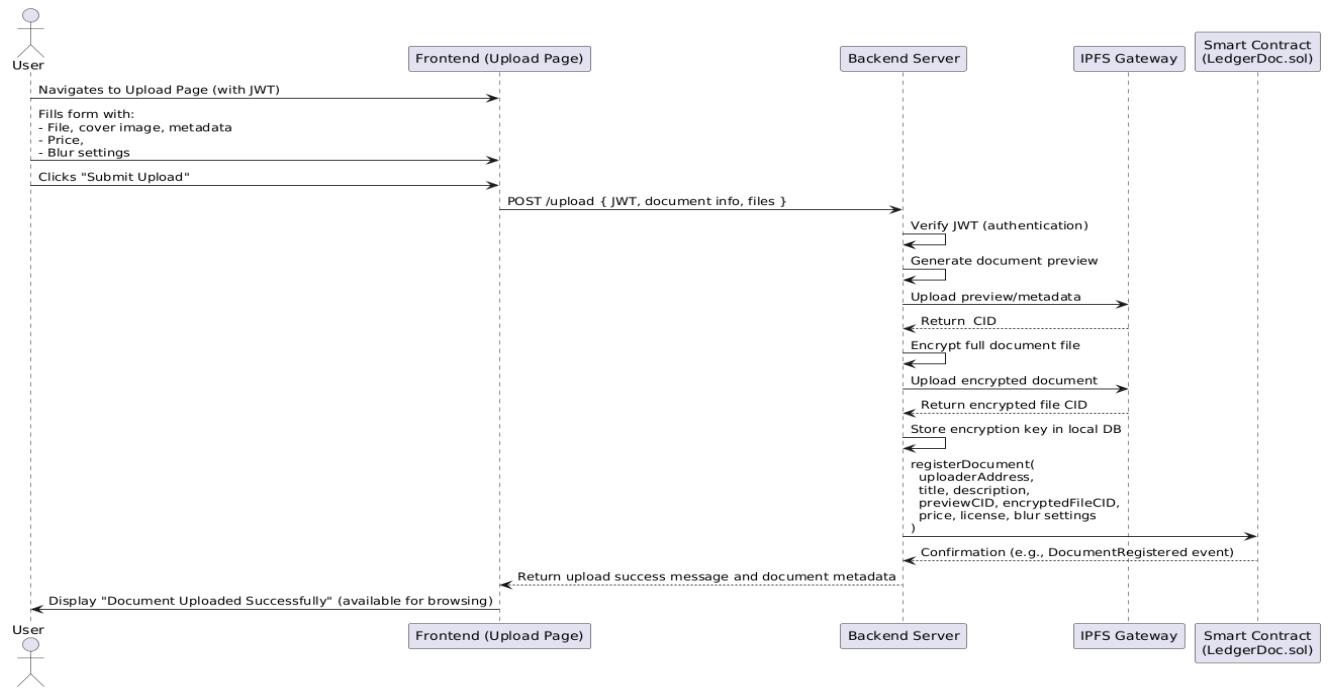


figure 9 Diagramme de séquence de téléchargement

### 3.3.2.3 Diagramme de séquence d'achat

Le diagramme de séquence de la figure 13 illustre le processus complet d'achat et d'accès à un document sur la plateforme. Après authentification, l'utilisateur peut parcourir ou rechercher des documents et effectuer un achat via MetaMask. Une fois le paiement confirmé sur la blockchain, le document devient accessible depuis le tableau de bord de l'utilisateur. Lors de la demande d'accès, le backend vérifie l'achat et renvoie de manière sécurisée la clé de déchiffrement AES, permettant ainsi de déchiffrer le fichier et de le consulter ou de le télécharger localement.

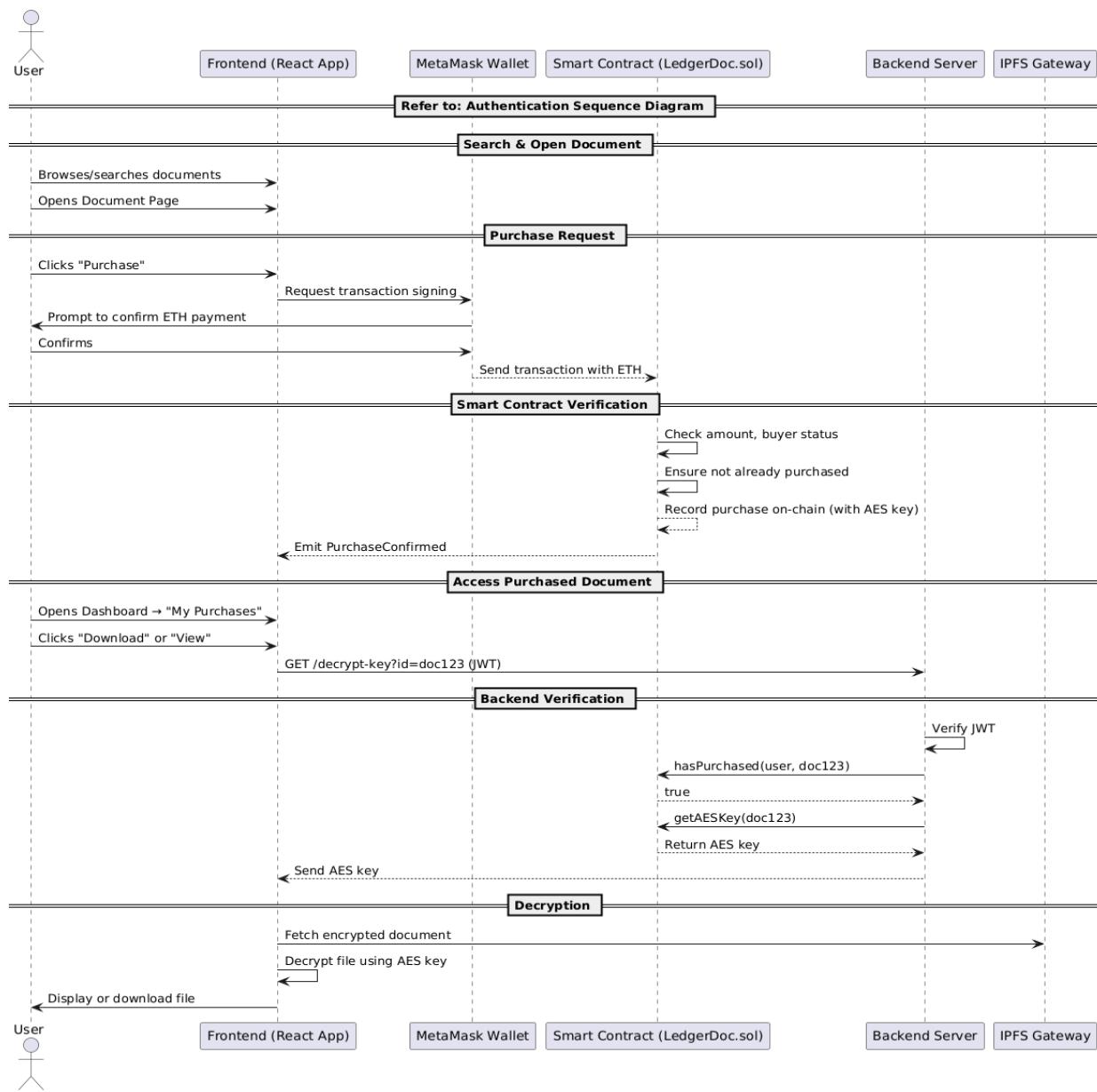


Figure 10 Diagramme de séquence d'achat

### 3.3.3 Diagramme de classes

Le diagramme de classes présenté dans la figure 14 modélise la structure principale du système de place de marché décentralisée de documents numériques, en mettant en évidence les entités clés et leurs relations.

L'Admin hérite des caractéristiques de l'utilisateur tout en disposant de priviléges supplémentaires, comme l'autorisation des fournisseurs ou la gestion des documents.

---

Les **Utilisateurs** interagissent avec la plateforme pour acheter, consulter ou téléverser des documents, après avoir authentifié leur portefeuille via **MetaMask**, qui assure la signature des transactions sur la blockchain.

Chaque **Document** est représenté par un ensemble de CIDs IPFS, incluant les versions chiffrées, les vignettes et les aperçus. Ces documents sont liés à un identifiant unique, à une catégorie, un prix, un nombre de téléchargements ainsi qu'à une note globale basée sur les évaluations des utilisateurs.

Les **Achats**, enregistrés sur la blockchain, relient un utilisateur à un document spécifique et permettent un contrôle d'accès sécurisé via des clés de déchiffrement. Enfin, le contrat intelligent LedgerDoc.sol de notre projet centralise la logique métier : il gère les utilisateurs, les autorisations, l'enregistrement des documents, ainsi que la validation des achats, assurant ainsi la transparence et l'immuabilité des opérations.

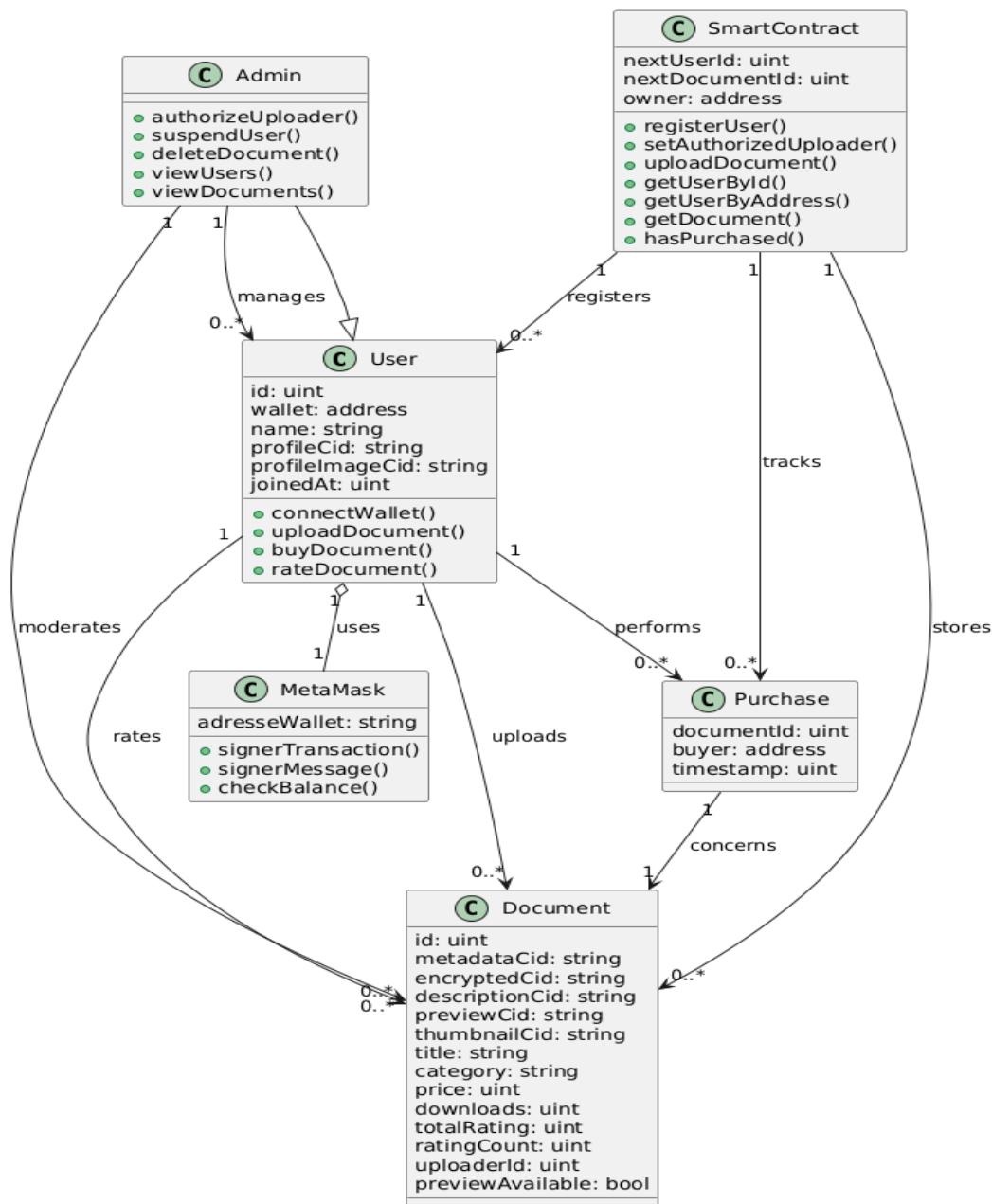


Figure 11 Diagramme de classes

---

## Conclusion

En somme, la phase d'analyse et de conception s'est révélée essentielle pour structurer notre projet de plateforme décentralisée de partage et de vente de documents numériques. L'élaboration des différents diagrammes UML nous a permis de formaliser les fonctionnalités principales du système, de l'authentification par portefeuille à la publication et à l'achat de documents sécurisés via la blockchain. Cette modélisation détaillée a posé les bases solides du développement, en clarifiant les rôles des utilisateurs (vendeur, acheteur, administrateur), les processus métier (téléversement, achat, chiffrement), ainsi que l'interaction entre les composants techniques (smart contract, IPFS, MetaMask, backend).

La suite de ce document présentera plus en détail les choix technologiques effectués pour concrétiser cette architecture, notamment l'intégration de React, Node.js, Solidity et IPFS, ainsi que des aperçus d'interface utilisateur.

Ces éléments permettront d'illustrer comment la conception théorique se traduit concrètement sur le plan technique et fonctionnel, en assurant une cohérence globale entre la vision initiale et sa mise en œuvre finale.

---

# **Chapitre4 :**

## **Choix Technique**

---

## Introduction

Dans ce chapitre nous allons tout d'abord présenter la description de notre environnement de travail, les langages, les Framework ainsi que les outils utilisés pour l'implémentation. Pour pouvoir par la suite entamer la présentation de notre produit finale en explorant ses différentes interfaces.

Technologies et outils utilisés

En ce qui concerne cette partie nous allons présenter chacun des logiciels de programmation, langage de programmation, Frameworks, qu'on a utilisé lors du développement de notre plateforme.

### 4.1 Technologies et outils utilisés

#### 4.1.1 Développement de la blockchain et des contrats intelligents

➤ **Ethereum :**

Ethereum est une plateforme open source basée sur la technologie blockchain qui permet de créer et d'exécuter des applications décentralisées et des contrats intelligents



Figure 12 Ethereum

➤ **Solidity :**

Solidity est un langage de programmation orienté objet dédié à l'écriture de contrats intelligents. Il est utilisé pour implémenter des smart contrat sur diverses blockchains, notamment Ethereum. Il a été développé par Christian Reitwiessner, Alex Beregszaszi, Yoichi Hirai et plusieurs anciens contributeurs principaux d'Ethereum pour permettre l'écriture de contrats intelligents sur des plateformes de blockchain telles qu'Ethereum.



solidity

Figure 13 Solidity

---

### ➤ Hardhat

Hardhat est un environnement de développement conçu pour créer et tester des contrats intelligents Ethereum. Il permet aux développeurs de compiler, déployer et tester efficacement du code Solidity. Hardhat intègre un réseau Ethereum local pour un développement rapide. Il prend en charge les scripts JavaScript et TypeScript pour automatiser les flux de travail. Les développeurs peuvent simuler des transactions et extraire des blocs instantanément pendant les tests. Il offre des fonctionnalités de débogage avancées, telles que les traces de pile et la journalisation de la console. Hardhat fonctionne parfaitement avec des bibliothèques comme Ethers.js pour interagir avec les contrats. C'est un outil populaire dans l'écosystème Web3 pour la création d'applications décentralisées.



*Figure 14 Hardhat*

### ➤ MetaMask

MetaMask est un portefeuille numérique et une extension de navigateur permettant d'interagir avec la blockchain Ethereum et d'autres réseaux compatibles EVM. Il sert d'interface entre les utilisateurs et les applications décentralisées (dApps), facilitant la gestion des comptes, la signature des transactions et la connexion aux plateformes Web3. Développé par ConsenSys, MetaMask est devenu un outil incontournable pour les utilisateurs et développeurs dans l'écosystème blockchain, offrant à la fois simplicité et sécurité.



*Figure 15 MetaMask*

---

### ➤ Piñata

Piñata est une plateforme Web3 qui facilite la gestion et l'hébergement de fichiers sur le réseau décentralisé IPFS. Elle permet aux développeurs de stocker, partager et sécuriser des contenus (images, vidéos, métadonnées) grâce au pinning, garantissant leur disponibilité. Très utilisée dans l'écosystème NFT, Piñata offre des API et une interface simple pour intégrer facilement un stockage décentralisé aux applications Web3.



Figure 16 Piñata

### 4.1.2 Backend

#### ➤ Node.js

Node.js est un environnement JavaScript puissant, parfait pour le Web3. Avec son moteur V8, il permet de développer des API décentralisées et d'interagir avec les blockchains. Son architecture asynchrone optimise la création de dApps et smart contracts, grâce à des librairies comme ethers.js. Intégrant facilement Ethereum et IPFS, Node.js s'appuie sur l'écosystème npm pour des solutions Web3 performantes



Figure 17 Node.js

#### ➤ Express.js

Express.js est un Framework web minimaliste et flexible pour Node.js, conçu pour simplifier le développement d'applications serveur et d'API REST. Grâce à sa syntaxe intuitive et son système de middleware, il permet de gérer facilement les requêtes HTTP, les routes et les réponses. Crée par TJ Holowaychuk et maintenu par la Node.js Fondation, Express.js est devenu la base de nombreuses applications web modernes, alliant légèreté et performances.



Figure 18 Express.js

---

## ➤ Ethers.js

Ethers.js est une bibliothèque JavaScript permettant d'interagir avec la blockchain Ethereum. Elle permet de se connecter à des nœuds, de lire ou écrire des données, de signer et envoyer des transactions, et d'interagir avec des contrats intelligents. Légère et facile à utiliser, elle est largement adoptée dans le développement d'applications Web3



Figure 19 Ethers.js

### 4.1.3 Interface utilisateur

- **React.js**

React.js est une bibliothèque JavaScript performante et flexible, créée par Meta (ex-Facebook). Elle permet de développer des interfaces dynamiques avec une expérience utilisateur fluide, soutenue par une communauté open source active. Compatible avec Windows, MacOs et Linux, React prend en charge JavaScript, TypeScript et JSX (un mélange de HTML et JS).

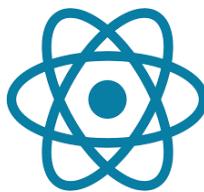


Figure 20 React.js

- **Tailwind CSS**

**Tailwind CSS** est un Framework CSS utility-first qui permet de concevoir des interfaces utilisateur modernes et réactives directement dans le balisage HTML. Contrairement aux Frameworks traditionnels comme Bootstrap, Tailwind offre des classes atomiques pour composer des designs sur mesure sans écrire de CSS personnalisé.



Figure 21 Tailwind CSS

---

#### 4.1.4 Environnement de développement

- **Visual Studio Code**

**Visual Studio Code (VS Code)** est un éditeur de code source léger, mais puissant, développé par Microsoft. Gratuit et open-source, il prend en charge une multitude de langages de programmation et offre des fonctionnalités avancées comme le débogage, la complétion intelligente, la gestion de Git intégrée et un terminal embarqué. Grâce à son système d'extensions, VS Code est hautement personnalisable et s'adapte à tous les workflows, du développement web à l'analyse de données.



Figure 22 VS Code

- **Git**

**Git** est un système de contrôle de version distribué, open-source, conçu pour gérer efficacement les projets de développement logiciel. Il permet de suivre les modifications du code, de collaborer en équipe et de revenir à des versions antérieures si nécessaire.



Figure 23 git

## 4.2 ipfs

**InterPlanetary File System (IPFS)** est un protocole de stockage distribué qui vise à transformer la manière dont les fichiers sont partagés et accessibles sur Internet. Contrairement à l'approche traditionnelle du Web, où les fichiers sont localisés en interrogeant l'adresse IP d'un serveur distant (appelée adressage basé sur l'emplacement), IPFS adopte une méthode appelée adressage basé sur le contenu.

---

**Adressage basé sur l'emplacement :** les limites du Web traditionnel Dans l'infrastructure actuelle du Web, lorsqu'un utilisateur souhaite télécharger un fichier, il interroge une adresse précise qui pointe vers un serveur contenant le fichier. Si ce serveur est indisponible ou hors ligne, le fichier devient inaccessible, même si d'autres utilisateurs possèdent déjà une copie du même fichier. Cette dépendance à un point central de défaillance constitue une faiblesse majeure.

**Le principe d'IPFS :** adressage basé sur le contenu IPFS résoudre ce problème en identifiant chaque fichier à l'aide d'un hachage cryptographique unique dérivé de son contenu. Ce hachage agit comme une empreinte digitale du fichier. Ainsi, lorsqu'un utilisateur souhaite récupérer un fichier, il interroge le réseau IPFS en demandant ce hachage spécifique. Le réseau recherche alors ce contenu chez n'importe quel nœud (utilisateur) qui possède une copie, éliminant la nécessité d'un serveur centralisé.

## 4.3 Mécanisme de chiffrement et de déchiffrement AES

AES (Advanced Encryption Standard) est un algorithme de chiffrement symétrique couramment utilisé pour sécuriser les données numériques. Contrairement au chiffrement asymétrique, qui repose sur une paire de clés, AES utilise une seule clé secrète pour chiffrer et déchiffrer les fichiers, ce qui le rend à la fois rapide et efficace.

### Le chiffrement symétrique : une seule clé pour deux opérations

Dans ce modèle, le fichier est chiffré avec une clé secrète avant d'être stocké, et cette même clé est requise pour le déchiffrer. Cela implique une gestion rigoureuse de la distribution des clés afin d'assurer que seules les personnes autorisées puissent accéder au contenu protégé.

### Fonctionnement d'AES : un standard robuste

AES chiffre les fichiers par blocs de 128 bits à l'aide d'une clé de 128, 192 ou 256 bits. L'algorithme applique plusieurs tours de transformation selon la longueur de la clé (10, 12 ou 14 tours), rendant le fichier illisible sans la clé appropriée.

### Application dans notre système : chiffrement côté serveur

Dans notre plateforme , le processus de chiffrement est effectué côté serveur dès qu'un document est soumis pour la vente. Le serveur génère une clé AES unique, chiffre le fichier, puis le téléverse sur IPFS sous forme chiffrée. Seule la version chiffrée est accessible publiquement, ce qui empêche toute consultation non autorisée.

## Déchiffrement côté client : accès sécurisé après achat

Après avoir acheté un document, l'utilisateur obtient la clé AES via un canal sécurisé . Le fichier chiffré est alors téléchargé depuis IPFS, puis déchiffré localement dans le navigateur grâce à cette clé. Ce mécanisme garantit que seul l'acheteur puisse consulter le contenu original, même si celui-ci est stocké sur un réseau public et distribué.

## 4.4 Architecture Technique du Système

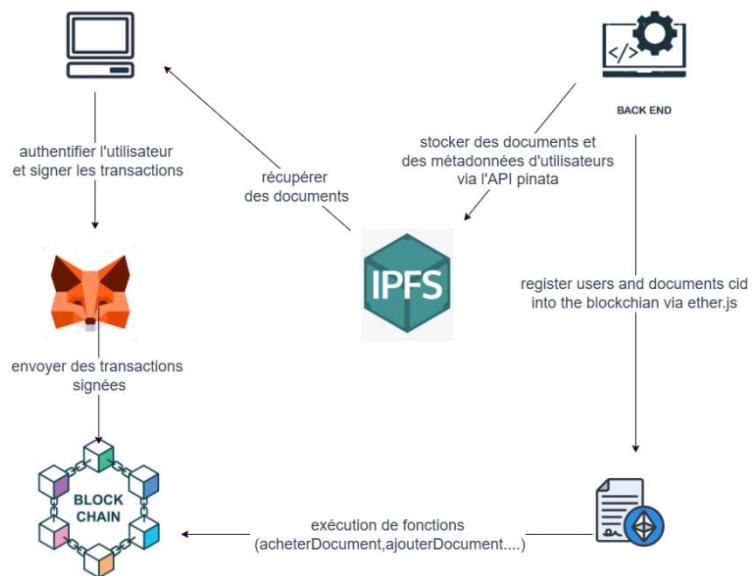


Figure 24 Architecture Technique

La figure 27 illustre l'architecture technique modulaire et décentralisée de l'application, une plateforme d'échange de documents numériques intégrant la technologie blockchain Ethereum, le stockage décentralisé via IPFS, un frontend moderne développé avec React, et une logique d'authentification sécurisée basée sur MetaMask et JWT.

Ce système repose sur l'interopérabilité entre les contrats intelligents, une interface web intuitive, et un backend Express léger facilitant la gestion des utilisateurs et des achats. Il offre un haut niveau de sécurité grâce à l'encryptions AES côté client, empêchant tout accès non autorisé aux fichiers.

---

#### 4.4.1 Module Utilisateur

Ce module gère l'inscription, l'authentification, les rôles, et l'activité des utilisateurs (vendeurs ou acheteurs).

- **Stack utilisée :** Express.js (backend Node.js), JWT (authentification), MetaMask (signature), IPFS
- **Fonctionnalités :**
  - Connexion via signature de message avec **MetaMask**
  - Attribution de **rôles** : acheteur, vendeur, administrateur
  - Tableau de bord personnalisé affichant les documents achetés, vendus, ou téléchargés
  - Enregistrement sécurisé des documents sur IPFS
  - Transmission de la **clé de déchiffrement AES** après achat confirmé

#### 4.4.2 Module Blockchain

Ce module repose sur un smart contract **Solidity** déployé sur le réseau Ethereum (testnet ou local), assurant la gestion transparente et décentralisée des documents et des transactions.

- **Contrat utilisé :** LedgerDoc.sol
  - Gestion des utilisateurs enregistrés
  - Enregistrement des documents : titre, catégorie, prix, CID IPFS
  - Suivi des achats, des téléchargements, et des évaluations
- **Interactions :**
  - Le frontend React utilise **Ethers.js** pour interagir avec le smart contract
  - Le backend surveille les événements « Purchase » émis par le contrat pour délivrer la clé AES à l'acheteur

---

#### **4.4.3 Module IPFS (Stockage Décentralisé)**

Les fichiers PDF des livres sont stockés sur IPFS (InterPlanetary File System), un système de fichiers distribué.

- **Fonction** : Fournir un accès sécurisé, immuable et décentralisé aux contenus numériques. Justification du choix d'IPFS :
- **Résilience** : les fichiers restent accessibles sans dépendre d'un serveur unique.
- **Scalabilité** : adapté à une croissance importante du nombre de livres.
- **Traçabilité immuable** : chaque fichier est associé à un identifiant unique (hash CID) enregistré sur la blockchain.

## **Conclusion**

Dans ce chapitre, nous avons présenté l'ensemble des technologies, langages et outils utilisés pour développer notre plateforme de vente et d'achat de documents numériques. Le projet repose sur l'intégration de contrats intelligents Ethereum, de stockage décentralisé via IPFS, d'un système de chiffrement côté client et d'une interface web moderne construite avec React. Nous avons également intégré un backend Node.js pour la gestion de l'authentification et la distribution des clés de déchiffrement, ainsi qu'un assistant intelligent pour améliorer l'expérience utilisateur.

L'architecture globale du système combine une interface réactive et intuitive, une infrastructure décentralisée sécurisée, ainsi que des mécanismes de contrôle d'accès intelligents. Cette approche garantit à la fois la sécurité des contenus, la transparence des transactions et la fiabilité du fonctionnement de la plateforme.

---

## Chapitre 5 :

### Réalisation

---

## **Introduction**

Ce chapitre est entièrement dédié à la présentation détaillée de l'application développée. Nous allons explorer en profondeur les différents aspects de cette solution, en mettant en avant ses fonctionnalités principales, son architecture technique, son interface utilisateur moderne, ainsi que les avantages qu'elle propose en matière de sécurité, transparence et simplicité d'utilisation.

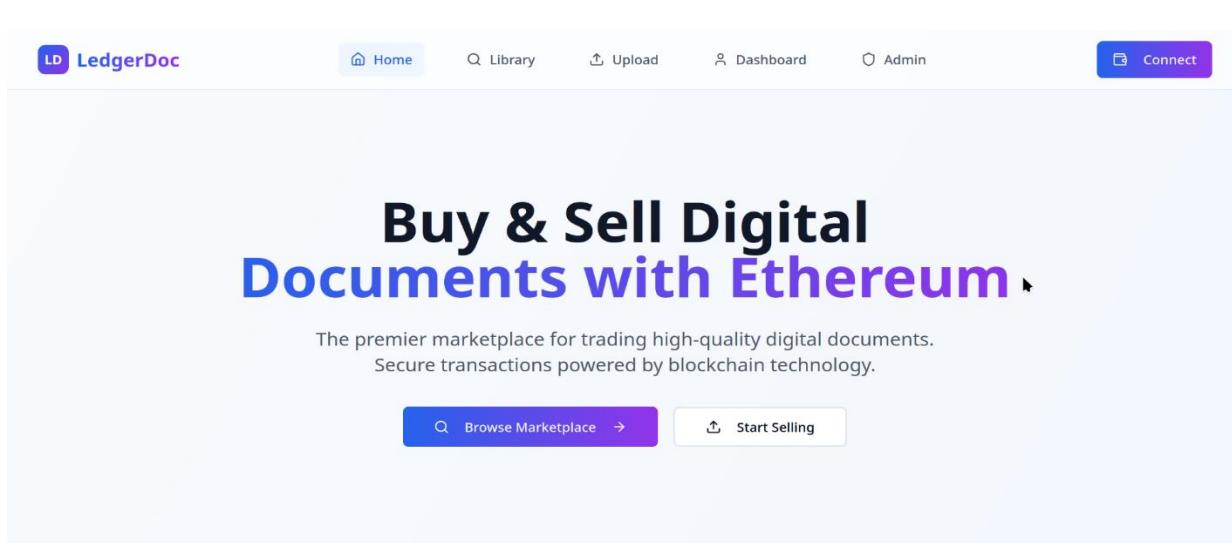
### **5.1 Mise en œuvre de l'application**

Dans cette section, nous allons présenter les captures d'écran de notre application, en expliquant en détail chaque étape du processus. Chaque capture d'écran sera accompagnée d'une explication claire et concise des fonctionnalités présentées.

#### **5.1.1 Démonstration utilisateur**

##### **1. Page d'accueil :**

La page d'accueil présente une introduction claire et synthétique à la plateforme, permettant aux utilisateurs de comprendre rapidement son objectif et son fonctionnement général.



This screenshot shows the 'Why Choose LedgerDoc?' section of the website. It features a title 'Why Choose LedgerDoc?' and a subtitle 'Secure, fast, and reliable document trading'. A blue speech bubble icon is in the top right. Below this, there are three cards: 'Secure Ethereum Payments' (with a lock icon), 'Protected Content' (with a shield icon), and 'Instant Downloads' (with a lightning bolt icon). Each card has a brief description: 'All transactions secured by blockchain technology with MetaMask integration', 'Your documents are secured and only accessible after purchase verification', and 'Get immediate access to purchased documents with our fast delivery system'. A large blue speech bubble icon is at the bottom right.

Figure 25 Page d'accueil 1

The screenshot shows the LedgerDoc homepage. At the top, there is a navigation bar with the logo "LD LedgerDoc", "Home", "Library", "Upload", "Dashboard", and "Admin". Below the navigation bar is a secondary navigation menu with categories: Education, Templates, Legal, Code, Design, Finance, Research, and Marketing. The main content area features a section titled "Trending Documents" with three cards. The first card is for "Complete Web3 Development Guide" (Education, 1200 downloads, 0.05 ETH price). The second card is for "Smart Contract Templates" (Code, 850 downloads, 0.03 ETH price). The third card is for "DeFi Investment Strategies" (Finance, 650 downloads, 0.08 ETH price). A "View All Documents" button is located below these cards. A blue horizontal bar runs across the bottom of the page.

This screenshot shows the same LedgerDoc homepage as above, but with a prominent purple banner at the top. The banner has the text "Ready to Get Started?" and "Join thousands of creators and buyers trading digital documents securely on the blockchain". It includes two buttons: "Connect Your Wallet" and "Upload Your First Document". The rest of the interface is identical to the first screenshot, including the navigation bar, secondary menu, and trending documents section.

The screenshot shows the footer of the LedgerDoc website. It includes the "LD LedgerDoc" logo, a brief description of the platform, and links to "Library" (Browse Documents, Sell Documents, Dashboard) and "Support" (Contact Us, FAQ, Wallet Help). On the right side, there are links to "Legal" (Terms of Service, Privacy Policy) and a "Support" icon (a blue circle with a white question mark). A small URL "http://localhost:8080/upload" is also visible.

Figure 26 . Page d'accueil 2

## 2. Authentification :

pour la partie connexion, il vous suffit d'appuyer sur le bouton de connexion, puis une fenêtre MetaMasque apparaît vous demandant la permission de signer un message qui sera utilisé pour vérifier votre identité dans le backend,

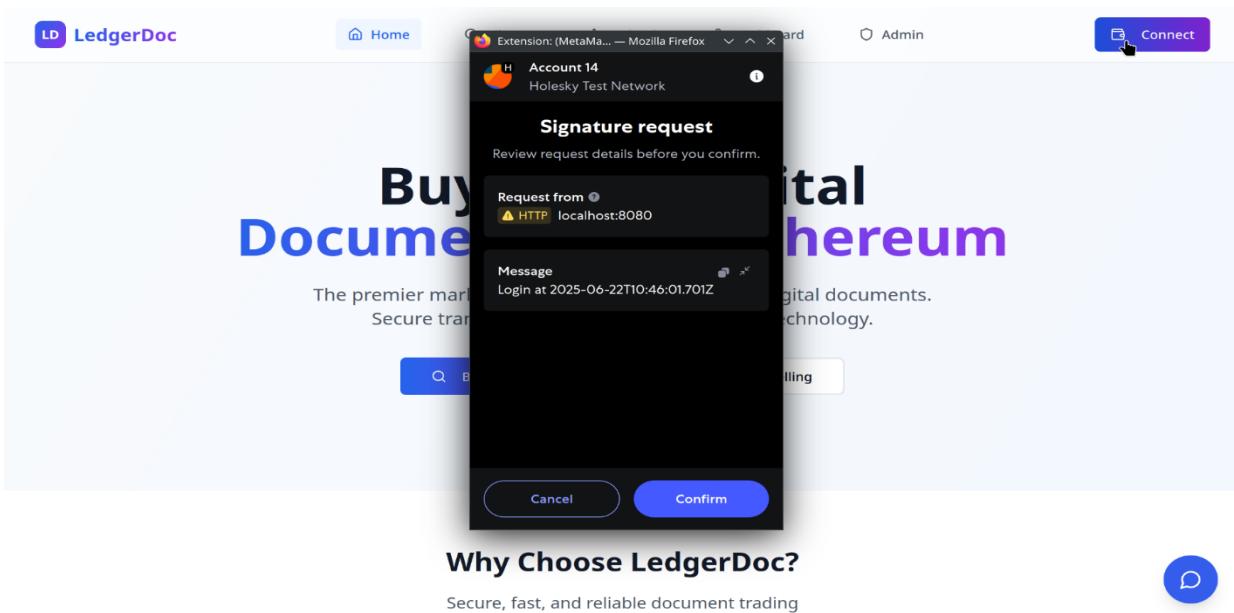
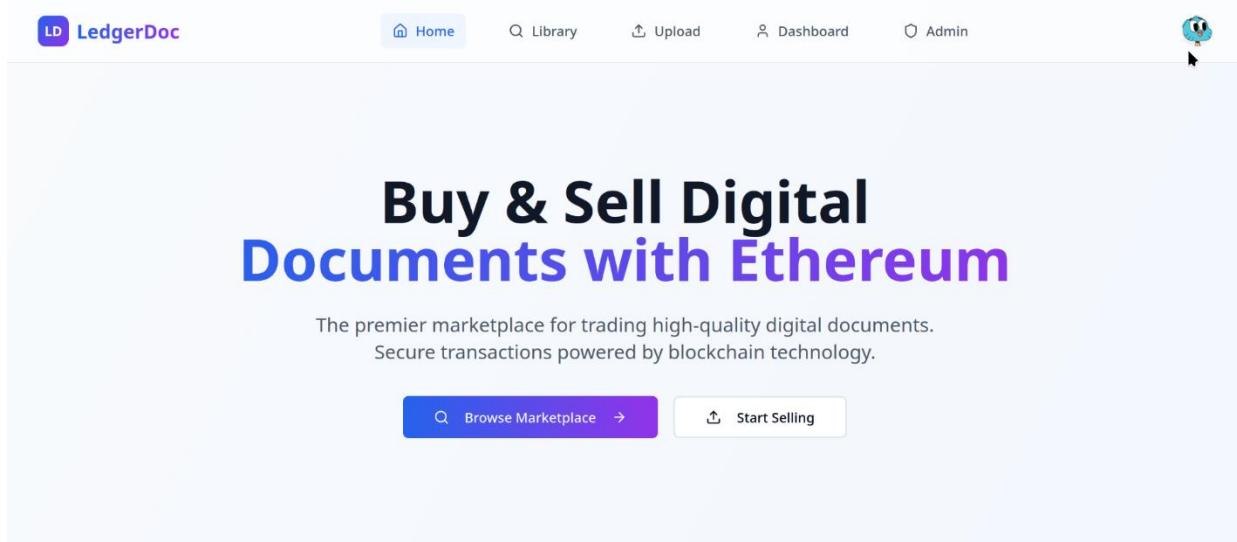


Figure 27 Authentification

Après une connexion réussie votre profil est chargé



### Why Choose LedgerDoc?

Secure, fast, and reliable document trading



### 3. La bibliothèque

C'est là que vous pouvez naviguer et rechercher des documents

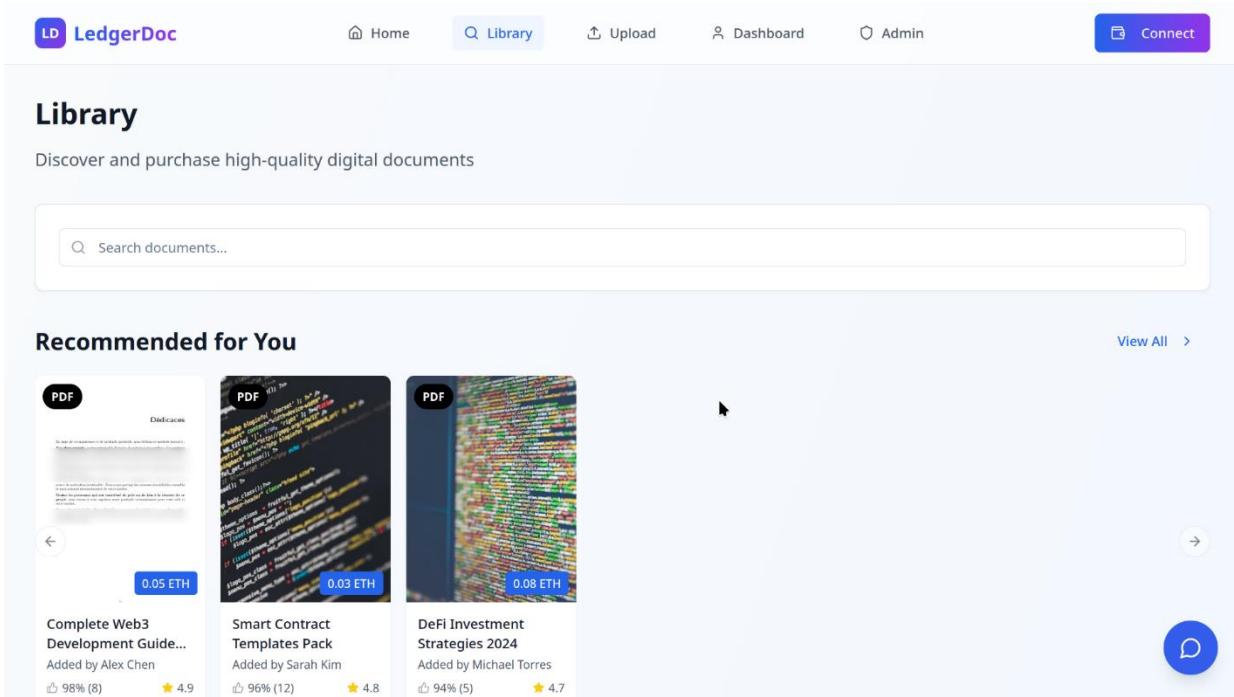


Figure 28 bibliothèque

## 4. Dashboard

C'est ici que vous trouverez vos documents achetés/ouverts à l'achat et des informations générales sur vos documents

The screenshot shows the LedgerDoc dashboard interface. At the top, there is a navigation bar with links for Home, Library, Upload, Dashboard (which is highlighted in blue), and Admin. A user icon is also present. Below the navigation bar, the title "Dashboard" is displayed, followed by the sub-instruction "Manage your documents and track your performance".

The main content area features several cards:

- Overview:** Shows "Total Earnings \$ 0.0 ETH (~\$6,127.50 USD)".
- Purchases:** Shows "Total Sales 0 +12% from last month".
- My Documents:** Shows "Documents 0 3 active listings".
- Recent Sales:** Shows "Your latest document sales".
- Top Performing Documents:** Shows "Your best-selling documents".

The footer of the page contains links for support and legal information:

- LedgerDoc:** The logo and name.
- Library:** Browse Documents, Sell Documents, Dashboard.
- Support:** Contact Us, FAQ, Wallet Help.
- Legal:** Terms of Service, Privacy Policy.

Figure 29 Dashboard

## 4.1 Vos achats

The screenshot shows the "Purchases" section of the LedgerDoc dashboard. At the top, there is a navigation bar with links for Home, Library, Upload, Dashboard (highlighted in blue), and Admin. A user icon is also present. Below the navigation bar, the title "Dashboard" is displayed, followed by the sub-instruction "Manage your documents and track your performance".

The main content area shows a list of purchased documents:

- Geometric representation of two-qubit entang...**  
Author: Default\_Name (change me)  
Purchased: 2025-06-22  
Price: 0.01 ETH  
Buttons: View, Download
- Sequential Short-Text Classification with Recur...**  
Author: Default\_Name (change me)  
Purchased: 2025-06-22  
Price: 0.0 ETH  
Buttons: View, Download
- Revealing the Breakdown Mechanism and Heat...**

Figure 30 achats

## 4.2 Vos documents téléchargés

The screenshot shows the LedgerDoc dashboard interface. At the top, there is a navigation bar with links for Home, Library, Upload, Dashboard (which is highlighted in blue), and Admin. There is also a user profile icon. Below the navigation bar, the title "Dashboard" is displayed, followed by the subtitle "Manage your documents and track your performance". A horizontal menu bar includes Overview, Purchases, My Documents (which is highlighted in blue), and Sales History. A search bar labeled "Search documents..." and a button labeled "Upload New Document" are also present. The main content area is titled "My Documents" and contains a single document entry for "my\_uploaded\_document" which is marked as "Active". The document details show a price of 0.001 ETH, sales of 0, and earnings of 0.0 ETH. Action buttons for "View", "Download", and "Edit" are available next to the document entry. A large blue circular button with a white speech bubble icon is located in the bottom right corner of the dashboard area.

Figure 31 documents téléchargés

#### 4.4 Historique des ventes

The screenshot shows the LedgerDoc dashboard interface, similar to Figure 31 but with a different active tab. The navigation bar, search bar, and upload button are identical. The title "Dashboard" is at the top, followed by the subtitle "Manage your documents and track your performance". The horizontal menu bar includes Overview, Purchases, My Documents, and Sales History (which is highlighted in blue). A search bar labeled "Search sales..." is present. The main content area is titled "Sales History" and contains a section titled "All Sales". It displays a single sale entry for "my\_uploaded\_document". The sale details show a buyer address (0xf39Fd6e51aad88F6F4ce6aB8827279cffB92266), the date (2025-06-22), and a payment of 0.001 ETH marked as "Completed". A large blue circular button with a white speech bubble icon is located in the bottom right corner of the sales history area.

Figure 32 historique des ventes

---

## **5. page de téléversement (upload)**

C'est ici que vous remplissez les informations sur le document que vous souhaitez télécharger, il existe différentes options, notamment le choix du niveau de flou du document prévisualisé et le

**Upload Your Document**

Share your knowledge and earn ETH

**Document Information**

Fill in the details about your document. All fields are required for blockchain verification.

**Upload Document (PDF only)**

Click to upload or drag and drop  
PDF files only (max 50MB)

**Cover Image (Optional)**

Click to upload document cover image  
JPG, PNG, GIF (max 10MB)

**Document Details**

Figure 33 page de téléversement 1

Nombre de premières pages sans flou afin que vous puissiez donner un bref aperçu du document à toute personne souhaitant l'acheter.

**Cover Image (Optional)**

Click to upload document cover image  
JPG, PNG, GIF (max 10MB)

**Document Details**

**Document Title**

Enter a clear, descriptive title

**Description**

Describe what your document contains and who it's for

**Categories**

<input type="checkbox"/> Education	<input type="checkbox"/> Templates	<input type="checkbox"/> Legal	<input type="checkbox"/> Code
<input type="checkbox"/> Design	<input type="checkbox"/> Finance	<input type="checkbox"/> Research	<input type="checkbox"/> Marketing

Add custom category  +

Figure 34 page de téléversement 2

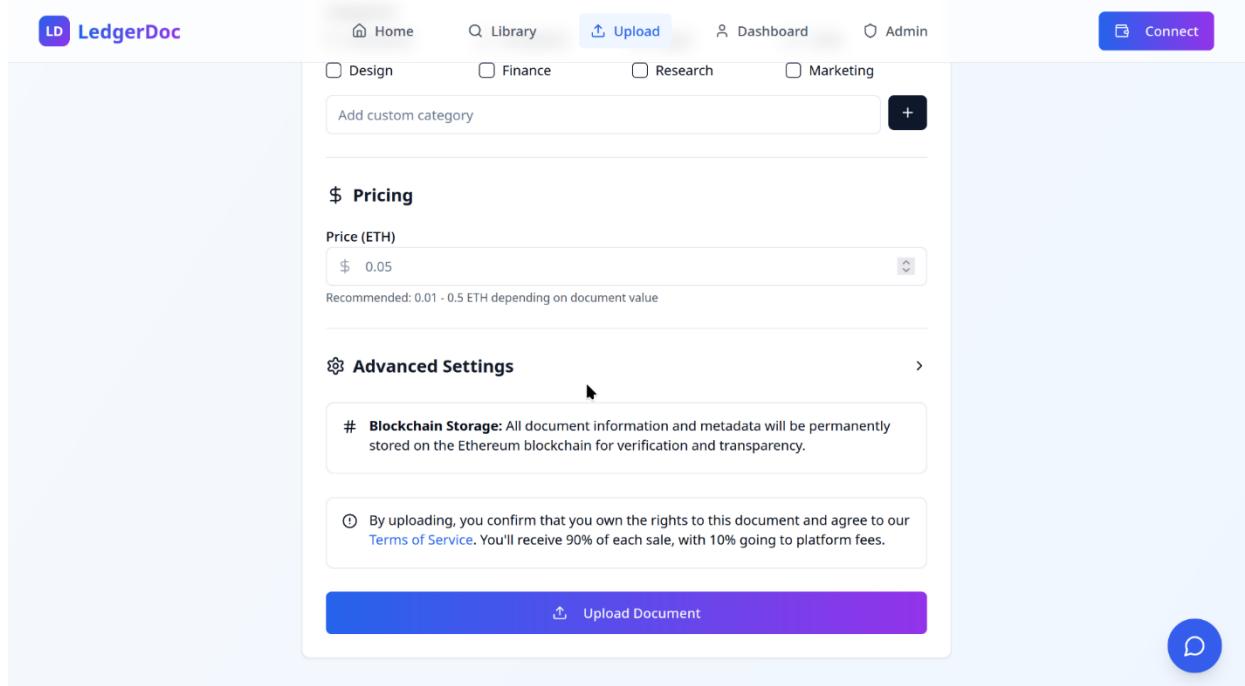


Figure 35 page de téléversement 3

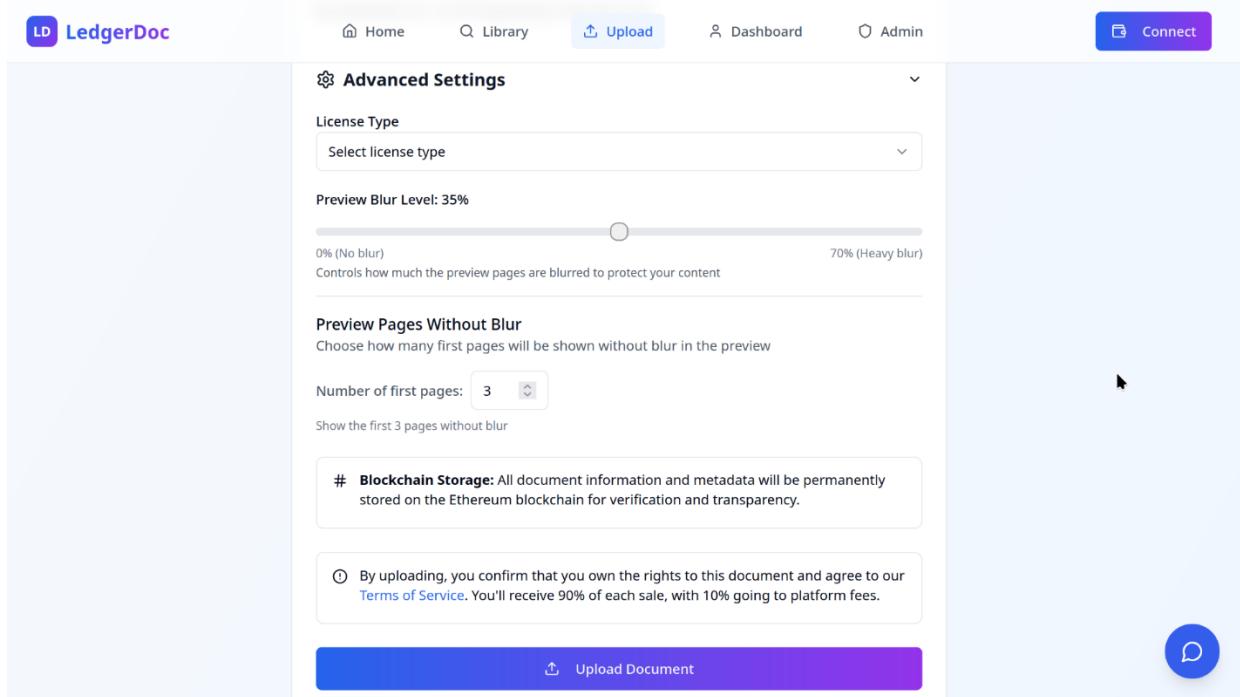


Figure 36 page de téléversement 4

## 5. page de profil où vous pouvez mettre à jour vos informations personnelles

The screenshot shows the 'Profile' section of the LedgerDoc application. At the top, there's a navigation bar with icons for Home, Library, Upload, Dashboard, Admin, and a user icon. Below the navigation is a sub-navigation bar for 'Profile' with links for Account Information, Personal Information, and Activity.

**Personal Information:** This section allows users to update their personal details. It includes fields for 'Full Name' (stof) and 'Email Address' (bennasser.offic@gmail.com). There's also a link to 'Edit Profile'.

**About Me:** This section indicates 'No description available.'

**Account Details:** Shows the address 0x5DF5c9d509097145f04B24D8B9e64549f3adFc8F and the fact that the user is a 'Member since June 2025'.

Figure 37 page de profil 1

This screenshot shows the 'Your Uploaded Documents' section of the profile page. It lists two documents: 'pfe\_v1.pdf' and 'table\_des\_matières-1-2.pdf'. Both documents are marked as 'Active' with a price of '0.001 ETH', '0' sales, and '0.0 ETH' earnings. Each document has a circular icon with an eye symbol next to it.

Document	Status	Price	Sales	Earnings
pfe_v1.pdf	Active	0.001 ETH	0	0.0 ETH
table_des_matières-1-2.pdf	Active	0.001 ETH	0	0.0 ETH

Figure 38 page de profil 2

## 5.1.2 Démonstration administrateur

The screenshot shows the Admin Dashboard of the LedgerDoc platform. At the top, there are navigation links: Home, Library, Upload, Dashboard, Admin, and a user icon. Below the header, a section titled "Admin Dashboard" with a shield icon says "Manage users and moderate content". It displays three main statistics boxes:

- Total Users: 4 All registered users
- Total Documents: 11 All uploaded documents
- Total Transactions: 0 Document purchases

Below these boxes are two tabs: "User Management" and "Content Moderation". Under "User Management", there is a sub-section titled "User Management" with the sub-instruction "Manage user accounts, view statistics, and handle suspensions". A search bar contains the address "0x5DF5c9d509097145f04B24D8B9e64549f3adFc8F". A user profile card for "stof" (address 0x5DF5c9d509097145f04B24D8B9e64549f3adFc8F) is shown, indicating 4 documents and 0.0117 ETH, with status "Suspended". Buttons for "View" and "Activate" are present, along with a blue message icon.

la page administrateur où il peut voir les statistiques générales de la plateforme, et gérer les utilisateurs et les documents

figure 39 page d'admin 1

The screenshot shows the Admin Dashboard interface. At the top, there are three cards: 'Total Users' (4), 'Total Documents' (12), and 'Total Transactions' (0). Below these are two tabs: 'User Management' and 'Content Moderation'. The 'Content Moderation' tab is active, displaying a search bar with the query 'ion with Recurrent and Convolutional Neural Networks'. A result card for 'Sequential Short-Text Classification with Recurrent and Convolutional Neural Networks' by stof is shown, with options to 'View', 'Download', or 'Remove'. A blue message bubble icon is visible in the bottom right corner.

Figure 40 page d'admin 2

### 5.1.4 Achat

Pour acheter un document, vous pouvez le rechercher et y accéder, puis après avoir vu l'aperçu du document, vous pouvez cliquer sur le bouton acheter pour obtenir le document

The screenshot shows a document preview page for 'Geometric representation of two-qubit entanglement witnesses.pdf'. The document is categorized under Education, Quantum Dynamics Theory, and Physics. It has a rating of 0.0 (0 reviews) and is 0 pages long. The file size is 8440v2 [quant-ph] 10 Jul 2015. A 'Purchase for 0.01 ETH' button is visible. To the right, a 'Document Preview' section contains the abstract and first few sections of the paper. A sidebar titled 'You might also like' shows a related document titled 'Smart Contract Security Audit Checklist' with a rating of 4.7 and a price of 0.02 ETH. A blue message bubble icon is visible in the bottom right corner.

Figure 41 page document 1

Figure 42 page document 2

Click de achat

Figure 43 page document 3

Puis tout ce qu'il faut attendre un peu pour que la transaction soit confirmée

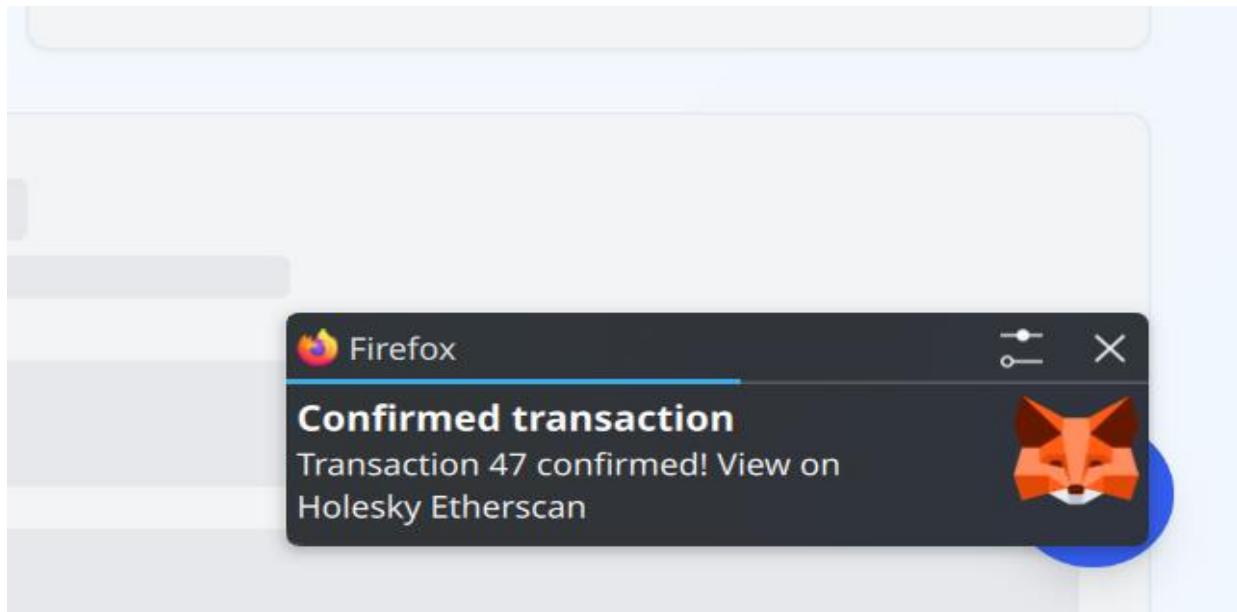


Figure 44 confirmation de transaction effectuée

## 5.2 Phase de test

### 5.2.1 Tests

Après l'intégration complète des composants du système incluant le frontend en React, les contrats intelligents déployés via Hardhat, l'interaction via Ethers.js, et le stockage décentralisé des fichiers sur IPFS une phase de test rigoureuse a été conduite pour valider le bon fonctionnement de l'ensemble. Les tests réalisés sont détaillés comme suit :

- **Tests unitaires** : Chaque module a été testé séparément pour garantir sa conformité. Les fonctions critiques du smart contract (comme l'achat ou l'enregistrement) ont été vérifiées avec des scripts automatisés. Les composants React ont été testés indépendamment pour valider l'affichage et le comportement.
- **Tests d'intégration** : Ces tests ont permis de vérifier la communication entre les différentes couches : interface React, appels vers Ethers.js, interaction avec le contrat intelligent, enregistrement des fichiers sur IPFS, et récupération post-achat. Quelques problèmes de synchronisation ont été détectés, puis corrigés.
- **Tests de performance** : Le système a été testé dans des conditions simulant plusieurs utilisateurs effectuant des achats ou consultations de documents. Malgré la latence liée à la blockchain, l'interface est restée fluide grâce à une gestion asynchrone des appels.

- 
- **Tests d'utilisabilité** : Des utilisateurs ont testé l'interface pour évaluer sa clarté et sa facilité d'utilisation. Ces retours ont permis d'améliorer la navigation, les messages d'erreur, et la logique de parcours utilisateur.
  - **Tests d'interopérabilité** : L'interaction entre le backend Node.js, les smart contracts, et IPFS (via Pinata) a été vérifiée pour assurer une communication cohérente entre tous les services.

## 5.2.2 Limitations

Malgré les tests approfondis et les améliorations apportées, certaines limitations ont été identifiées et méritent d'être mentionnées :

- **Absence de version mobile native**

Actuellement, l'application est responsive mais ne dispose pas d'une version mobile native Android/iOS. Cela pourrait limiter l'expérience des utilisateurs mobiles, notamment pour la lecture en mobilité ou l'accès hors-ligne. Le développement futur d'une application mobile dédiée est envisagé.

- **Dépendance à MetaMask**

L'authentification repose exclusivement sur MetaMask ou des portefeuilles Ethereum compatibles. Les utilisateurs non familiers avec le Web3 peuvent rencontrer des difficultés d'installation ou de compréhension du processus de connexion, ce qui peut freiner l'adoption initiale.

- **Limitations du stockage sur IPFS**

Bien que les fichiers soient stockés de manière décentralisée, leur disponibilité dépend du nombre de nœuds qui les hébergent. Sans pinning actif (via un service comme Pinata), un document peu consulté pourrait devenir temporairement inaccessible. Cela soulève des enjeux de persistance à long terme.

## Conclusion

Cette phase de test a permis de garantir une grande partie de la fiabilité du système et de révéler les points d'amélioration à envisager dans les itérations futures. Malgré certaines limitations techniques, les performances obtenues montrent que l'application est globalement stable, sécurisée, et prête à être déployée dans un environnement réel ou académique. Par ailleurs, la

---

phase de réalisation a constitué une étape centrale du projet. Elle a impliqué le développement des contrats intelligents, l'intégration de l'interface utilisateur avec la blockchain via Web3, la mise en place de l'hébergement décentralisé des fichiers via IPFS, ainsi que la conception d'une interface interactive sous React. Ce travail a permis de construire une base fonctionnelle et évolutive pour notre plateforme des documents numériques, en assurant une bonne cohérence entre les différentes couches techniques du système

## Conclusion et perspectives

Ce rapport présente le travail réalisé dans le cadre de mon projet de fin PFE du filière développement et base de données à université Chouaib Doukkali d'El Jadida, consistant en la conception et le développement d'une plateforme de marché numérique pour documents basés sur blockchain

Les principaux apports de ce projet sont les suivants :

- Une étude approfondie des technologies blockchain, notamment la plateforme Ethereum, ainsi que des systèmes de stockage décentralisé via IPFS, appliquées au commerce sécurisé de documents numériques.
- La conception d'une architecture intégrant smart contracts pour la gestion des utilisateurs, documents, transactions et évaluations, garantissant transparence, sécurité et immutabilité des échanges.
- La mise en place d'une interface utilisateur moderne et réactive avec React, intégrant la connexion via MetaMask, un tableau de bord complet, et une expérience utilisateur fluide pour la gestion et la consultation des documents.
- La création d'un espace d'administration permettant la gestion des utilisateurs (activation/suspension) et du contenu (suppression de documents), renforçant le contrôle et la modération de la plateforme.

Pour enrichir et faire évoluer notre système, plusieurs perspectives sont envisagées :

- Implémentation d'un système de réputation et récompenses sur blockchain, où les utilisateurs pourraient gagner des jetons ou badges pour leurs contributions, achats ou ventes, renforçant ainsi l'engagement et la confiance.
- Extension des fonctionnalités du chatbot IA pour proposer des recommandations personnalisées basées sur les historiques d'achat et de consultation.
- Amélioration de l'intégration des paiements en ETH et gestion automatique des transactions, avec une expérience utilisateur optimisée.
- Développement d'une application mobile native pour offrir un accès simplifié et sécurisé à la plateforme en mobilité.
- Mise en place de mécanismes avancés de watermarking et protection anti-piratage, pour garantir davantage la sécurité des documents distribués.

---

Cette plateforme innovante, alliant blockchain, stockage décentralisé pose les bases d'un écosystème sécurisé, transparent et performant pour l'échange de documents numériques, avec un fort potentiel d'extension pour répondre aux besoins futurs des utilisateurs.

---

# Bibliographie

1. Applications Décentralisées, [<https://journaldulcoin.com/lexique/dapp-application-decentralisee/>]
2. Architecture du projet, [<https://www.theserverside.com/tip/Introduction-to-Solidity-Build-an-Ethereum-smart-contract>]
3. Avantages UML, [<https://manureauxs.wp.imt.fr/2013/09/27/interet-de-luml-dans-un-projet-informatique/>]
4. Blockchain Hybride, [<https://academy.yellowcard.io/fr/glossary/consortium-blockchain/>]
5. Blockchain Privée, [<https://cdbf.ch/lexique/blockchain-privee/>]
6. Blockchain Publique, [<https://blockchain.gov.in/Home/BlockChain?blockchain=type>]
7. Échanges financiers, [<https://cryptoast.fr/comment-blockchain-peut-faciliter-échange-titres-financiers/>]
8. MetaMask, [<https://fr.wikipedia.org/wiki/MetaMask>]
9. ReactJS, [<https://www.50a.fr/0/react>]
10. Solidity, [<https://fr.wikipedia.org/wiki/Solidity>]
11. Pinata, [<https://pinata.cloud/>]
12. Technologie Blockchain, [<https://www.sap.com/france/products/artificial-intelligence/what-is-blockchain.html>]
13. Transferts d'argent et paiements, [<https://dumas.ccsd.cnrs.fr/dumas-02997638/document>]
14. UML, [<https://www.futura-sciences.com/tech/definitions/informatique-uml-3979/>]
15. Visual Studio Code, [[https://fr.wikipedia.org/wiki/Visual\\_Studio\\_Code](https://fr.wikipedia.org/wiki/Visual_Studio_Code)]
16. Web3, [<https://fr.wikipedia.org/wiki/Web3>]