Projet Web3 - DApp de Cartes de Collection Numeriques

1. Introduction et Contexte

Ce projet s'inscrit dans le cadre du developpement d'une application decentralisee (DApp) exploitant les principes du Web3. L'objectif est de concevoir une plateforme permettant la gestion et l'echange d'actifs numeriques sous forme de tokens, en respectant des contraintes metier specifiques.

La blockchain choisie pour ce projet est Ethereum, avec l'utilisation du framework Hardhat pour le developpement et les tests des smart contracts. Les metadonnees des ressources seront stockees sur IPFS afin de garantir leur perennite et leur decentralisation.

---

2. Presentation du Cas d'Usage

2.1 Concept General

Le cas d'usage retenu est un **marche decentralise de cartes de collection numeriques** de type trading cards. Les utilisateurs peuvent collectionner des cartes representant des personnages, creatures ou objets avec differents niveaux de rarete. Ces cartes peuvent etre echangees entre joueurs selon des regles definies par les smart contracts.

2.2 Objectifs Fonctionnels

- Permettre aux utilisateurs de posseder des cartes numeriques uniques et verifiables
- Offrir un systeme d'echange securise et transparent entre joueurs
- Garantir l'authenticite et la rarete de chaque carte
- Tracer l'historique complet de propriete de chaque carte
- Empecher la duplication frauduleuse et la speculation abusive

---

3. Justification de l'Utilisation de la Blockchain

L'utilisation de la blockchain pour ce projet se justifie par les principes fondamentaux suivants :

3.1 Decentralisation

Aucune autorite centrale ne controle le marche. Les echanges s'effectuent directement entre utilisateurs via des smart contracts, sans intermediaire. Cette approche elimine les risques lies a un point de defaillance unique.

3.2 Immutabilite

Une fois une carte creee ou un echange valide, l'information est inscrite de maniere permanente sur la blockchain. L'historique des transactions et des proprietaires ne peut etre ni modifie ni supprime, garantissant ainsi l'integrite des donnees.

3.3 Transparence

Toutes les transactions sont publiques et verifiables par quiconque. Les utilisateurs peuvent auditer le code des smart contracts et verifier les regles metier appliquees. Cette transparence renforce la confiance dans le systeme.

3.4 Securite

Les mecanismes cryptographiques de la blockchain garantissent que seul le proprietaire legitime d'une carte peut la transferer. Les smart contracts executent automatiquement les regles definies, eliminant les risques de fraude ou d'erreur humaine.

3.5 Rarete Verifiable

Contrairement aux systemes centralises ou l'editeur peut creer des copies a volonte, la blockchain permet de prouver mathematiquement la rarete d'une carte. Le nombre d'exemplaires est inscrit dans le smart contract et ne peut etre modifie.

---

4. Description des Ressources Tokenisees

4.1 Niveaux de Rarete

Chaque carte possede un niveau de rarete parmi les quatre categories suivantes :

Niveau	Nom	Valeur de Base	Disponibilite
1	Commune	10	Illimitee
2	Rare	50	Limitee
3	Epique	200	Tres limitee
4	Legendaire	1000	Ultra rare

La valeur de base determine le poids de la carte dans les mecanismes d'echange et permet d'etablir des equivalences entre cartes de raretes differentes.

4.2 Types de Cartes

Chaque carte appartient a l'un des quatre types thematiques suivants :

Type	Description
Guerrier	Personnages de combat, heros et combattants
Mage	Personnages magiques, sorciers et enchanteurs
Creature	Monstres, animaux mythiques et etres fantastiques
Artefact	Objets magiques, equipements et reliques

4.3 Attributs des Cartes

Chaque carte possede les attributs suivants :

Attribut	Type	Description
name	string	Nom unique de la carte
type	string	Type thematique
rarity	string	Niveau de rarete
value	uint	Valeur associee selon la rarete
power	uint	Statistique de puissance (1-100)
defense	uint	Statistique de defense (1-100)

---

5. Regles Metier

5.1 Regles d'Echange de Tokens

Echange Direct

Un utilisateur peut proposer une carte a un autre utilisateur en echange d'une de ses cartes. La transaction necessite la validation des deux parties pour etre executee.

Regles de Conversion

Un echange est considere comme equitable si les valeurs des cartes respectent un ratio maximum de 1:5. Cela signifie qu'une carte de valeur 10 peut etre echangee contre une carte de valeur 50 maximum. Au-dela de ce ratio, le smart contract refuse la transaction.

Exemples d'echanges valides :

- Carte Commune (10) contre Carte Commune (10) : ratio 1:1
- Carte Commune (10) contre Carte Rare (50) : ratio 1:5
- Carte Rare (50) contre Carte Epique (200) : ratio 1:4

Exemples d'echanges refuses :

- Carte Commune (10) contre Carte Epique (200) : ratio 1:20 (depasse 1:5)
- Carte Commune (10) contre Carte Legendaire (1000) : ratio 1:100 (depasse 1:5)

Validation des Transactions

Le smart contract effectue les verifications suivantes avant de valider un echange :

- Les deux utilisateurs possedent bien les cartes concernees
- Les regles de conversion sont respectees
- Les contraintes temporelles sont satisfaites

- Aucun des deux utilisateurs n'a atteint la limite de possession

5.2 Limites de Possession

Chaque utilisateur ne peut posseder que **4 cartes maximum** dans sa collection. Cette contrainte :

- Oblige les joueurs a faire des choix strategiques
- Favorise les echanges entre utilisateurs
- Empeche l'accumulation excessive par un seul joueur

Si un utilisateur possede deja 4 cartes et souhaite en acquerir une nouvelle, il doit prealablement echanger ou bruler l'une de ses cartes existantes.

5.3 Contraintes Temporelles

Cooldown entre Transactions

Un utilisateur doit attendre **5 minutes** entre deux transactions successives (echange ou acquisition). Cette contrainte :

- Empeche la speculation rapide
- Protege contre les attaques automatisees (bots)
- Laisse le temps aux utilisateurs de reflechir a leurs actions

Lock apres Acquisition

Apres avoir recu une nouvelle carte (par echange ou mint), celle-ci est verrouillee pendant **10 minutes**. Durant cette periode :

- La carte ne peut pas etre echangee
- La carte ne peut pas etre brulee
- La carte reste visible dans la collection du proprietaire

Ce mecanisme :

- Simule une periode de confirmation
- Securise les transactions contre les echanges en cascade
- Permet de detecter d'eventuelles anomalies

---

6. Format des Metadonnees

Les metadonnees de chaque carte sont stockees sur IPFS au format JSON. Voici la structure complete :

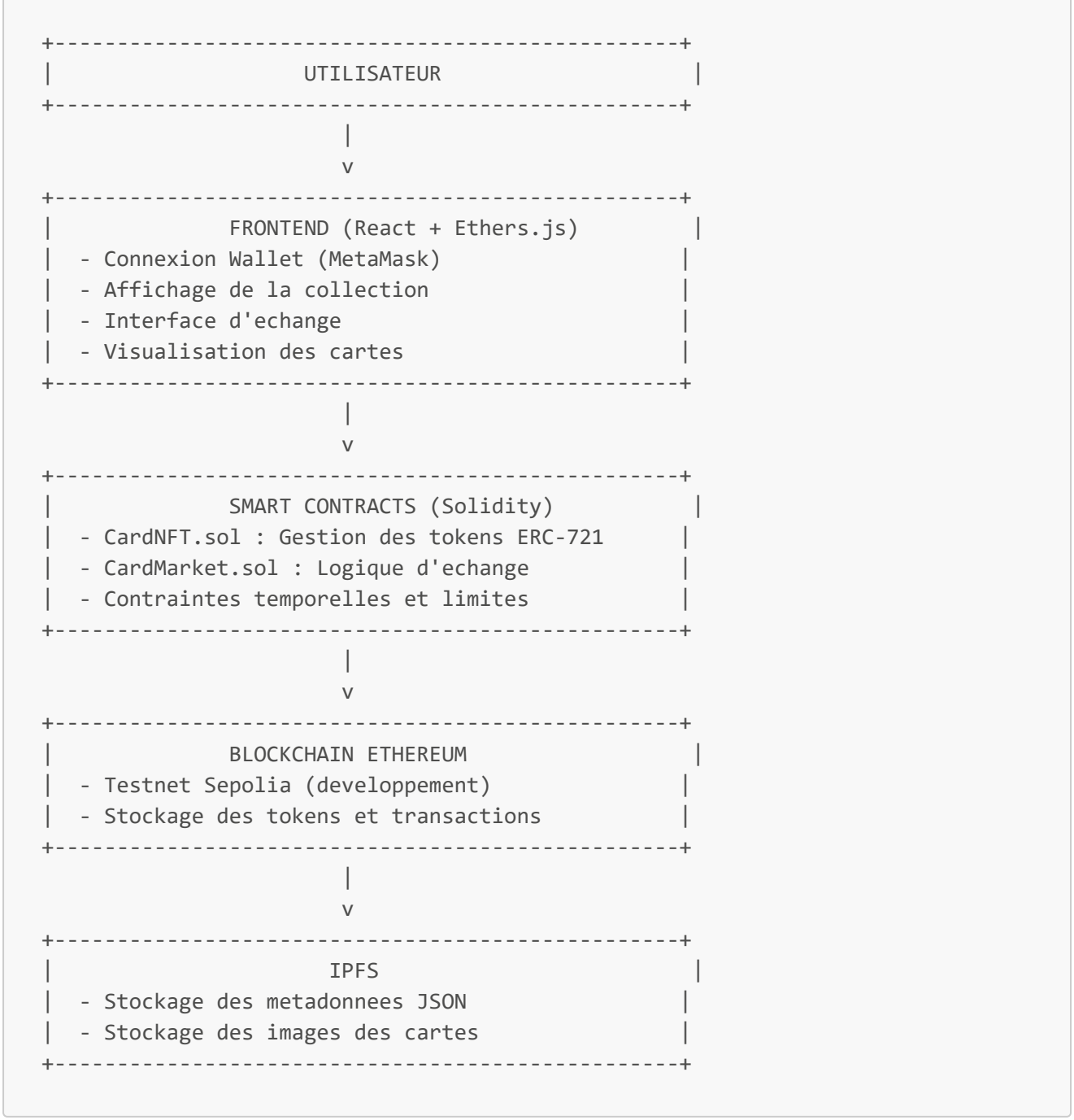
```
{
    "name": "Dragon des Abysses",
    "type": "Creature",
    "rarity": "Legendaire",
    "value": 1000,
    "power": 95,
```

```
    "defense": 80,
    "description": "Un dragon ancestral qui regne sur les profondeurs
marines.",
    "image": "ipfs://QmXxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
    "hash": "QmYyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy",
    "previousOwners": [
        "0x1234567890abcdef1234567890abcdef12345678",
        "0xabcdef1234567890abcdef1234567890abcdef12"
    ],
    "createdAt": 1706700000,
    "lastTransferAt": 1706750000,
    "edition": 1,
    "maxEdition": 10,
    "creator": "0x9876543210fedcba9876543210fedcba98765432"
}
```

Description des Champs

Champ	Type	Description
name	string	Nom unique de la carte
type	string	Type thematique (Guerrier, Mage, Creature, Artefact)
rarity	string	Niveau de rarete (Commune, Rare, Epique, Legendaire)
value	uint	Valeur associee selon la rarete
power	uint	Statistique de puissance (1-100)
defense	uint	Statistique de defense (1-100)
description	string	Description narrative de la carte
image	string	URI IPFS de l'image de la carte
hash	string	Hash IPFS du fichier de metadonnees complet
previousOwners	array	Liste des adresses des anciens proprietaires
createdAt	uint	Timestamp de creation (format Unix)
lastTransferAt	uint	Timestamp du dernier transfert
edition	uint	Numero d'edition de la carte
maxEdition	uint	Nombre maximum d'exemplaires pour cette carte
creator	address	Adresse du createur original de la carte

7. Architecture Fonctionnelle



8. Recapitulatif des Contraintes Techniques

Contrainte	**Implementation**
Tokenisation des ressources	Tokens ERC-721 avec 4 niveaux de rarete
Echanges de tokens	Smart contract avec ratio de conversion 1:5
Limites de possession	Maximum 4 cartes par utilisateur
Cooldown entre transactions	5 minutes entre deux operations
Lock apres acquisition	10 minutes de verrouillage
Stockage IPFS	Metadonnees et images sur IPFS

Contrainte	Implementation
Tests unitaires	Framework Hardhat avec couverture significative

9. Conclusion

Ce projet de marche decentralise de cartes de collection numeriques repond aux exigences du cahier des charges tout en proposant un cas d'usage concret et engageant. L'utilisation de la blockchain Ethereum garantit la securite, la transparence et l'immutabilite des transactions, tandis que le stockage sur IPFS assure la perennite des metadonnees.

Les regles metier definies (limites de possession, contraintes temporelles, regles d'echange) permettent de creer un ecosysteme equilibre qui favorise les interactions entre utilisateurs tout en empechant les abus.