PROJET DE DÉVELOPPEMENT BLOCKCHAIN

DAPP « JEUNE DIPLÔMÉ »

Problématique métier :

Nous sommes repartis de la problématique de **vérification de l'authenticité des diplômes délivrés par les établissements d'enseignement supérieur** à laquelle nous avons ajouté la problématique de **vérification de l'authenticité des évaluations de PFE** réalisées par les entreprises.

Ces 2 procédures de vérification sont essentielles pour le recrutement d'un jeune diplômé…

Pour plus d'informations sur les enjeux et objectifs du contrôle de faux diplôme(s) et la réussite du processus de vérification, vous pouvez lire l'article suivant :

- Comment reconnaître un faux diplôme ? Le fléau des recruteurs

Spécification de la DApp :

Périmètre fonctionnel : Registre de diplômes et d'évaluation des PFE et application de vérification de l'authenticité

Description (user stories) :

Cette application décentralisée offre les fonctionnalités suivantes :

- Un agent d'un établissement d'enseignement supérieur peut créer un compte pour son établissement qui va servir à enregistrer les jeunes diplômés et leurs diplômes.
- Un agent d'un établissement d'enseignement supérieur peut créer et sauvegarder un profil pour un étudiant lorsque ce dernier commence son stage de fin d'étude.
- Un agent d'un établissement d'enseignement supérieur peut ajouter un diplôme et mettre à jour les informations de son titulaire.
- Un agent de recrutement peut créer un compte pour son entreprise.
- Un agent de recrutement peut évaluer un étudiant en stage de fin d'étude et sera rémunéré en tokens.
- Un agent de recrutement peut acquérir des tokens pour le compte de son entreprise et qui vont servir au paiement des frais de la vérification de l'authenticité des diplômes.
- Un agent de recrutement peut vérifier l'authenticité d'un diplôme d'un candidat et paie les frais en tokens.

Acteurs :

- Établissement d'enseignement supérieur : Université, Faculté, école, institut…
- Tierce partie : Startup, entreprise...

Entités :

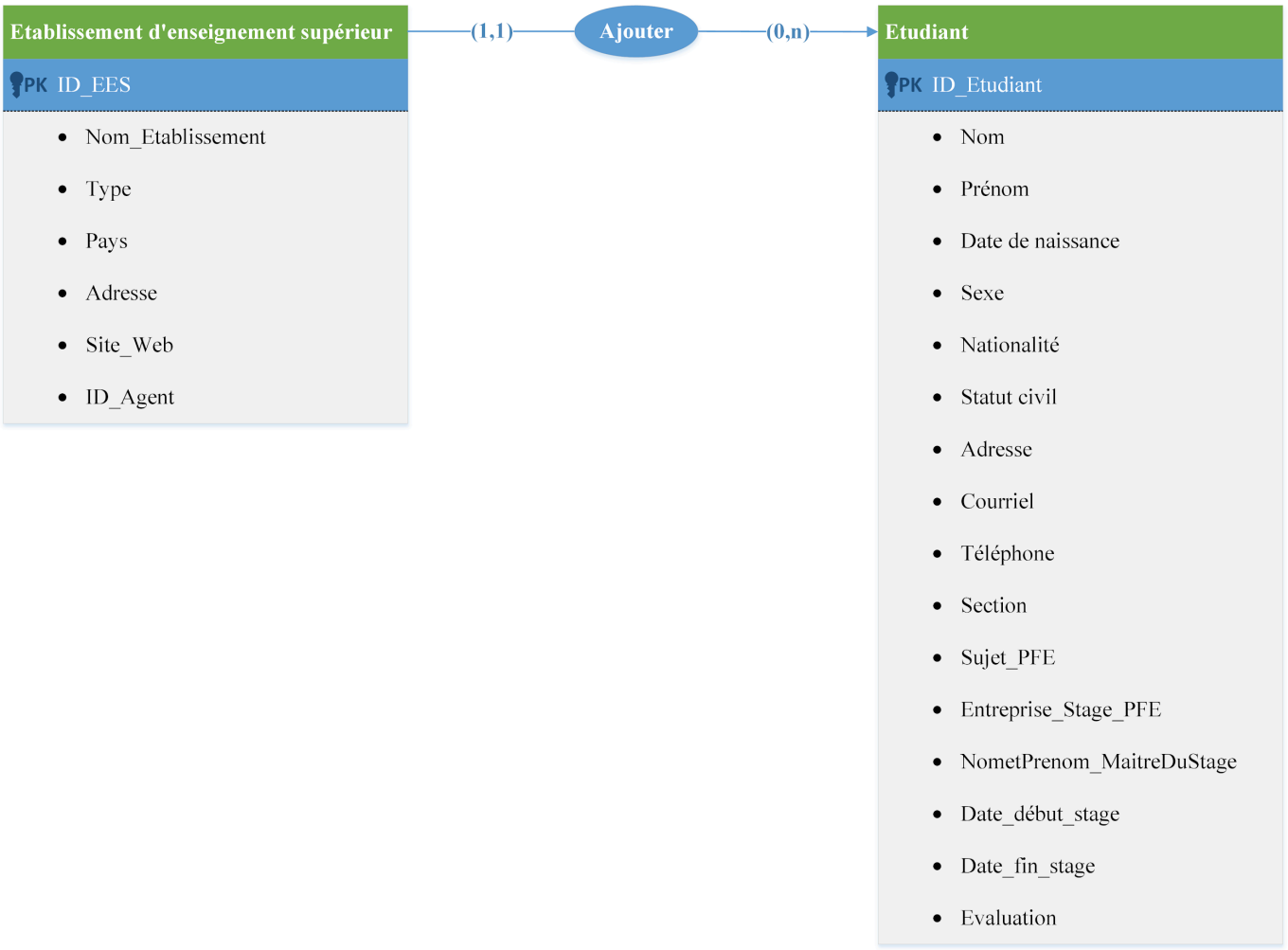


Diagramme entité association : Établissement-Étudiant

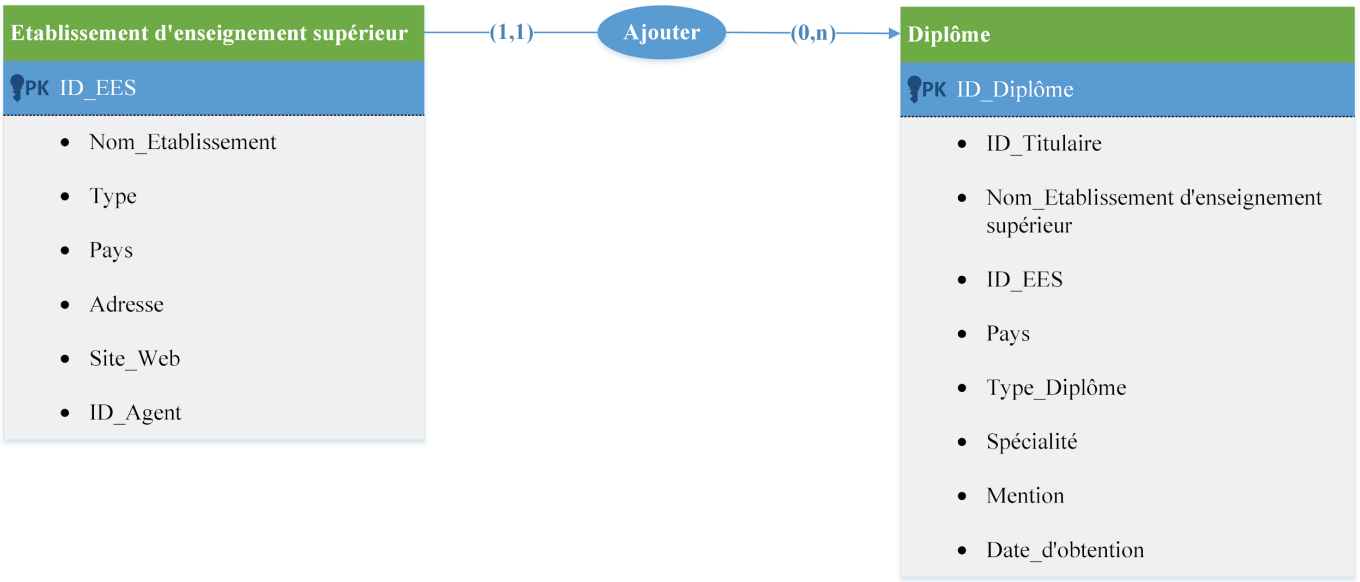


Diagramme entité association : Établissement-Diplôme

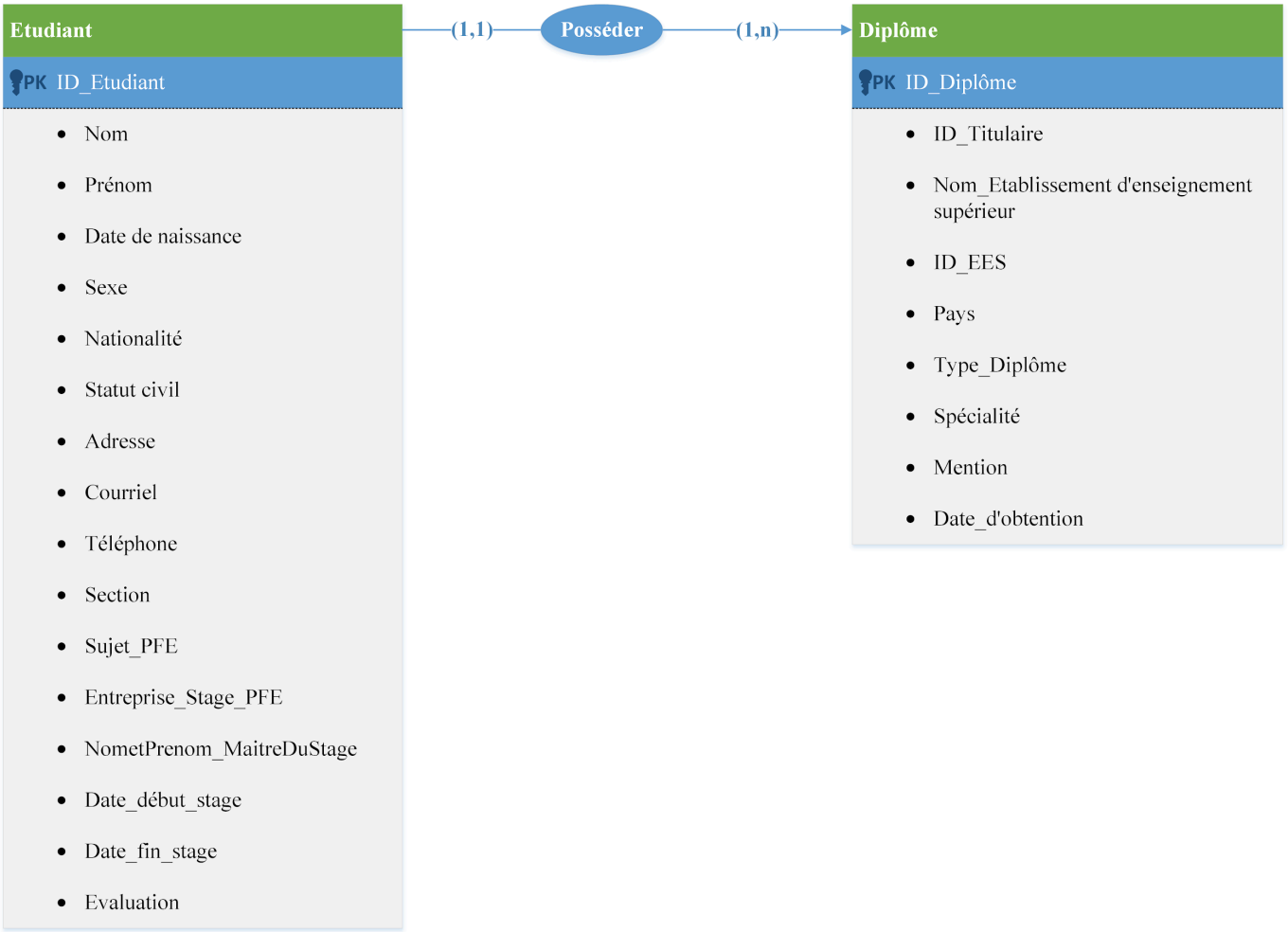


Diagramme entité association : Étudiant-Diplôme

Diagramme entité association : Entreprise-Étudiant

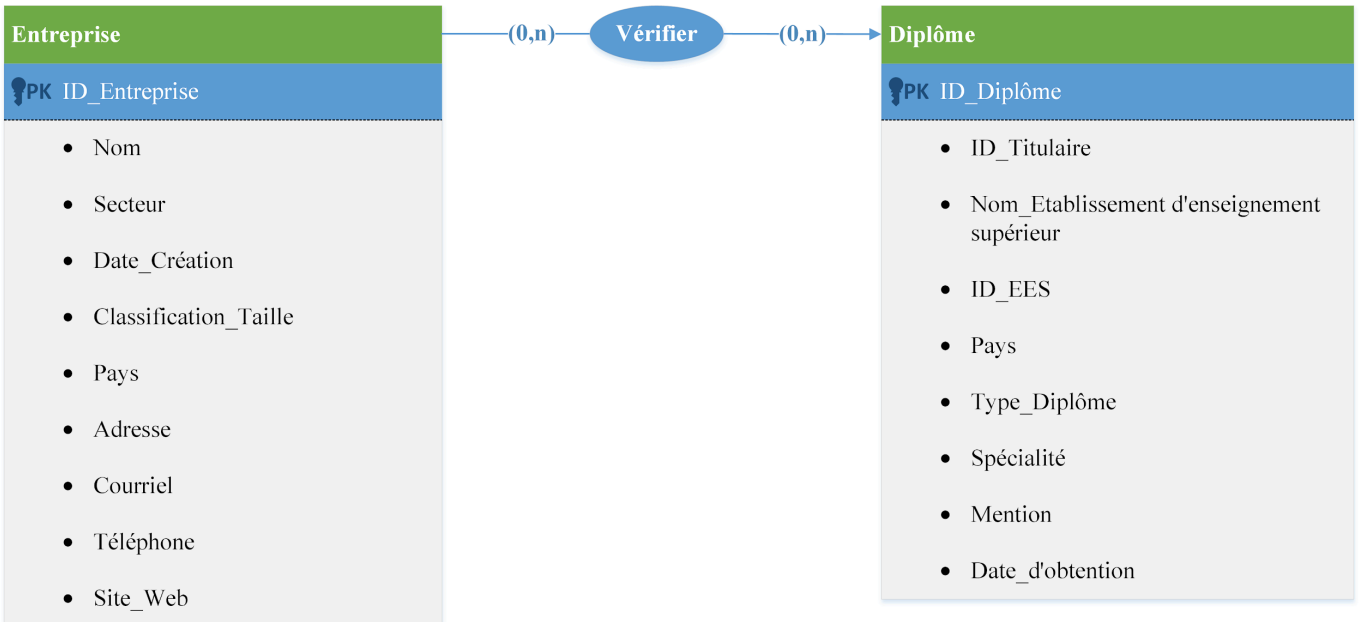
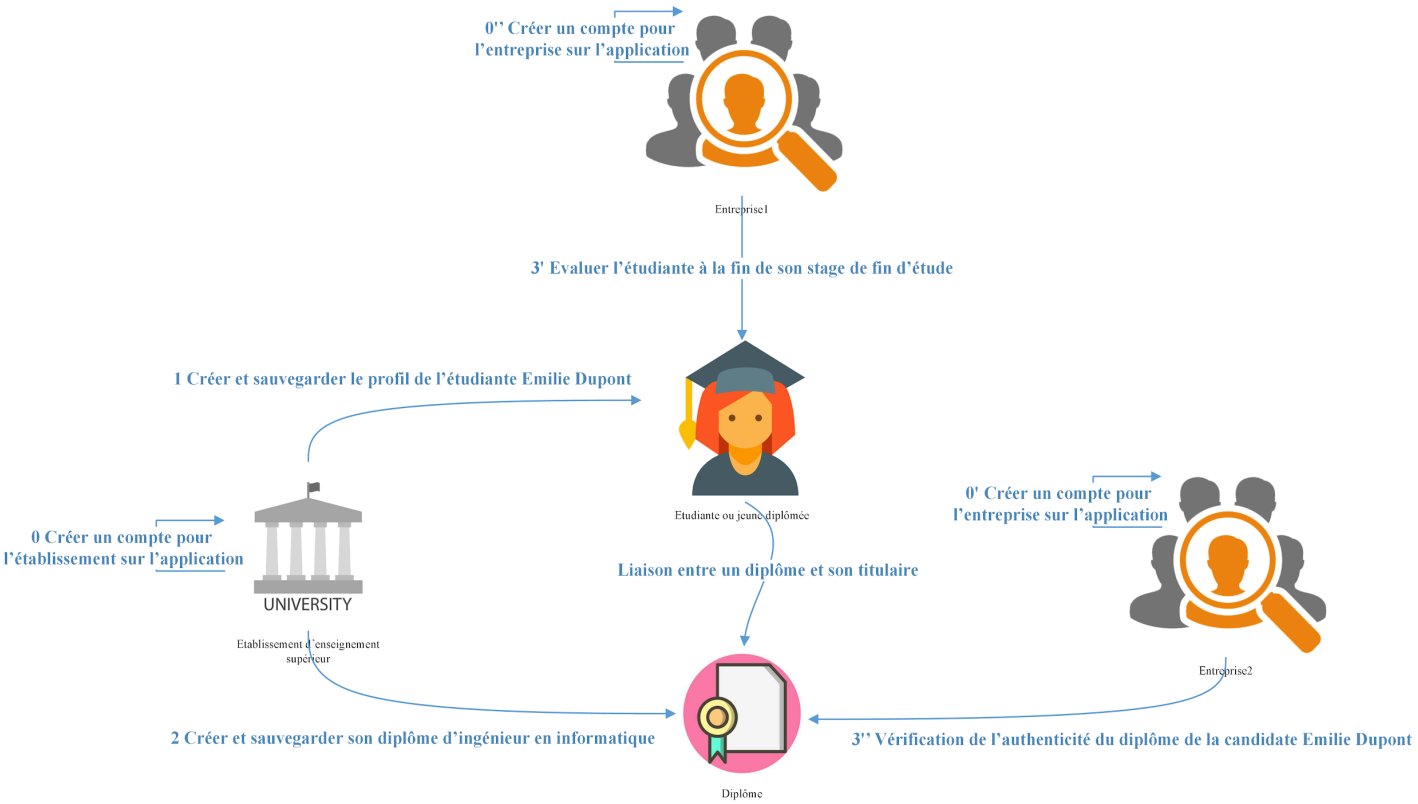


Diagramme entité association : Entreprise-Diplôme

Scénario d'utilisation de la DApp :



1. Description du jeton :

Un jeton ERC20 est couplé à l'utilisation de l'application. Il va servir au paiement des frais de vérification de l'authenticité des diplômes ainsi qu'à la rémunération des entreprises qui feront l'effort d'évaluer leurs stagiaires via l'application. L'échange des tokens est géré par les 3 transactions suivantes :

1. Transaction d'acquisition des tokens par les tierces parties : 0.01 Ether = 100 jetons
    a. On achète les tokens de chez celui qui a déployé la Dapp (qui est donc le propriétaire des tokens).
2. Transaction de rémunération des entreprises suite à l'évaluation de leurs stagiaires : 15 jetons par évaluation.
    a. Celui qui rémunère, c'est le propriétaire du jeton (celui qui a déployé l'application).
3. Transaction de paiement des frais de vérification : 10 jetons par vérification.
    a. Les frais sont à destination du smart contract de la Dapp (diploma).

2. NFT & Audit de sécurité

Diplômes sous forme de NFT
Afin d'augmenter l'unicité, la traçabilité et la portabilité des diplômes, ceux-ci doivent désormais être émis sous forme de jetons non fongibles (NFT) respectant le standard ERC-721.

Contraintes supplémentaires :

Chaque diplôme correspond à un NFT unique émis par un établissement d'enseignement. Le NFT contient les métadonnées essentielles du diplôme (nom de l'étudiant, nom du diplôme, établissement émetteur, date d'émission, identifiant unique). Les données sensibles ou volumineuses (comme une version PDF du diplôme) doivent être stockées sur IPFS avec un lien (CID) dans les métadonnées du NFT.

Le smart contract de NFT doit permettre :

La vérification de l'émetteur (seuls les établissements vérifiés peuvent minter un NFT).
Le changement de propriétaire (dans le cas d'un transfert symbolique vers un wallet personnel du diplômé).
L'immutabilité des données critiques une fois le NFT émis.

3. Audit de sécurité des smart contracts avec Mythril

Avant le déploiement sur un réseau public de test, les participants doivent effectuer une analyse de sécurité automatisée de leurs smart contracts à l'aide de l'outil Mythril.

Objectifs :
Identifier les vulnérabilités connues telles que :
Reentrancy
Integer overflow/underflow (si pas de SafeMath)
Front-running
Transaction-ordering dependence
Manque de restriction d'accès
Utilisation incorrecte de delegatecall

Générer le rapport d'audit Mythril (myth analyze).

Proposer et implémenter des contre-mesures aux vulnérabilités détectées :

Utilisation de OpenZeppelin pour les primitives sécurisées (ReentrancyGuard, Ownable, Pausable, SafeERC20, etc.). Implémentation de modificateurs de rôle et de contrôles stricts dans les fonctions sensibles.