## Révisions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Date de version** | **Version** | **Section et titre** | **N° page** | **Résumé des changements** | **Auteurs** |
| 06/03/2017 | 1.0 | Tous | Tous | Document initial | Sylla Mohamed  Baweu D. Marcel  Tchokonte Martin |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Contexte

À la fois monnaie cryptographique et véritable alternative aux monnaies traditionnelles, Bitcoin présente une innovation majeure en proposant un modèle de preuve en lieu et place des modèles classiques reposant sur la délégation de confiance.

Bitcoin est tout à la fois un système de paiement, une monnaie et une infrastructure de notariat électronique, à même de protéger l'intégrité et l'antériorité de nos données sensibles.

Bitcoin est indépendant de tout organisme, banque, banque centrale ou état. Entièrement libre et transparent, il est une infrastructure communautaire et open-source. Le grand apport de Bitcoin est de nous offrir ce « livre magique » avec la technologie blockchain.

En appréhendant les concepts et mécanismes de Bitcoin, nous nous efforcerons de mettre en place un système de paiement peer-to-peer à l'image du système Bitcoin inventé par Satoshi Nakamoto dans ce cours de programmation par composants.

# Modèle de classes métier

## Diagramme de classe

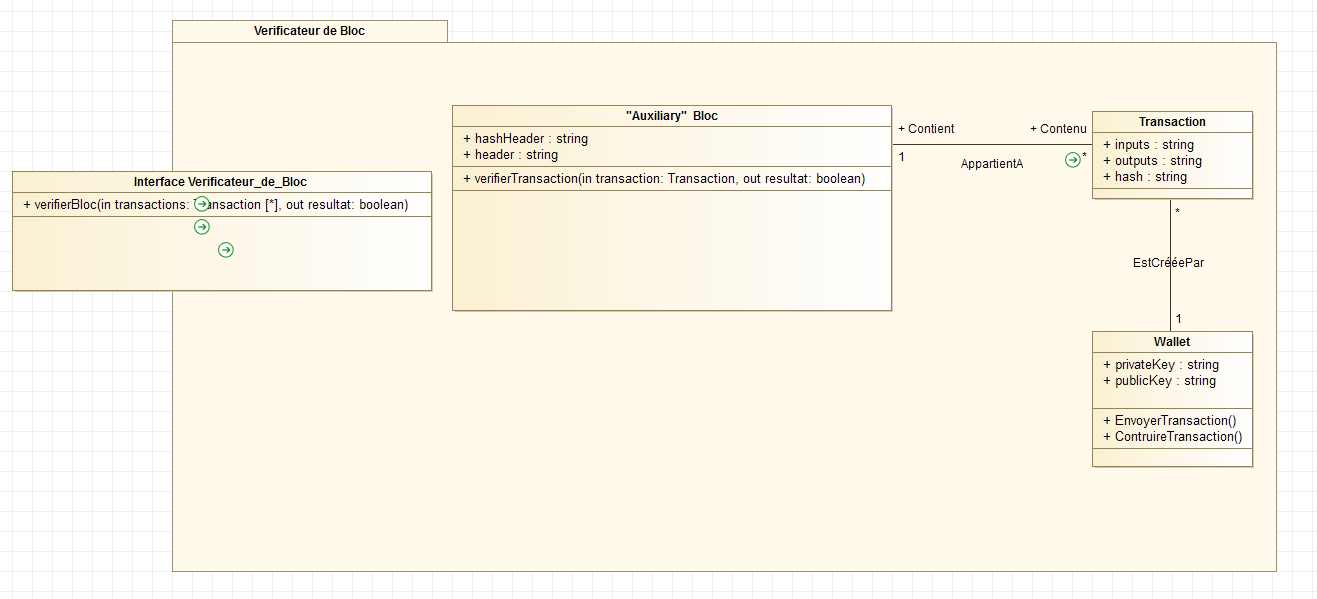
# Architecture de la couche métier

Nous allons décrire le paquetage concernant le "Vérificateur de blocs ".

## Vérificateur de bloc

Le paquetage Vérificateur de bloc possède comme classe auxiliaire la classe Bloc. Cette dernière appartient au paquetage ??? .

Le design pattern montre l'ensemble des fonctionnalités couvertes par le vérificateur de blocs.



## Les cas d'utilisation lié à la vérification d'un bloc

**Nom :** Système de vérification de bloc.

**Description**: Une fois une transaction validée, celle-ci sera envoyée au réseau Bitcoin pour être prise en compte. Une transaction Bitcoin est composée de deux parties :

* Des **« entrées »,** qui font référence à des Bitcoin enregistrés dans la blockchain et dont on possède les clefs de déverrouillage,
* Des **« sorties »**, composées d’adresses protégées par des verrous, vers lesquelles seront envoyés les Bitcoins spécifiés en « entrée »

Le réseau Bitcoin est composés de plusieurs milliers de nœuds, formant un réseau de type peer to peer dans lequel chaque nœud communique avec ses voisins :

**Acteurs** :

* Un bloc ....
* Une transaction ...
* Le mineur ...

|  |  |  |  |
| --- | --- | --- | --- |
| Étape | Action | Acteur | Résultat / Commentaire |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |