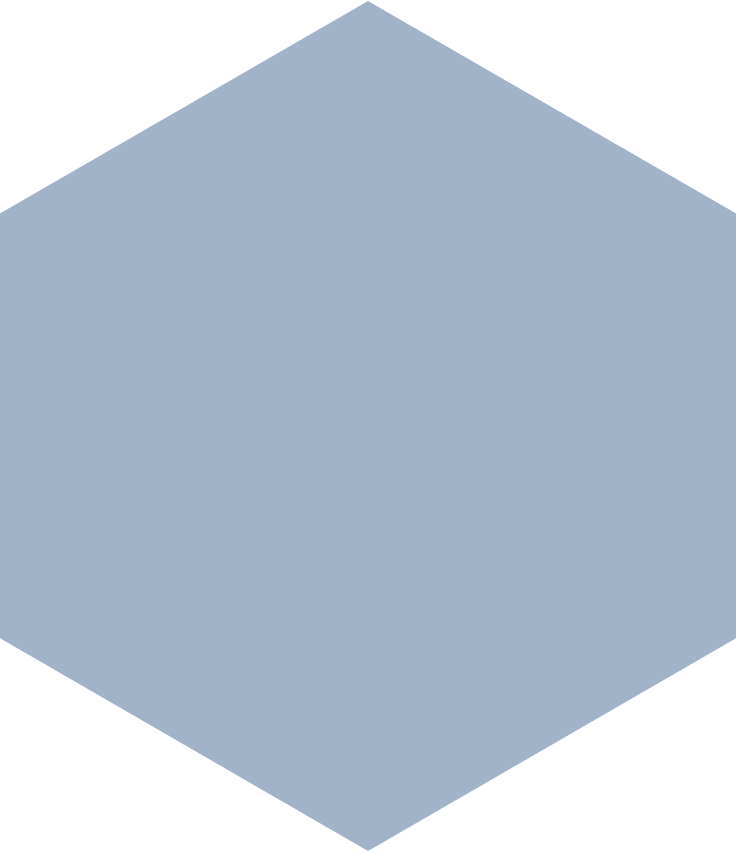
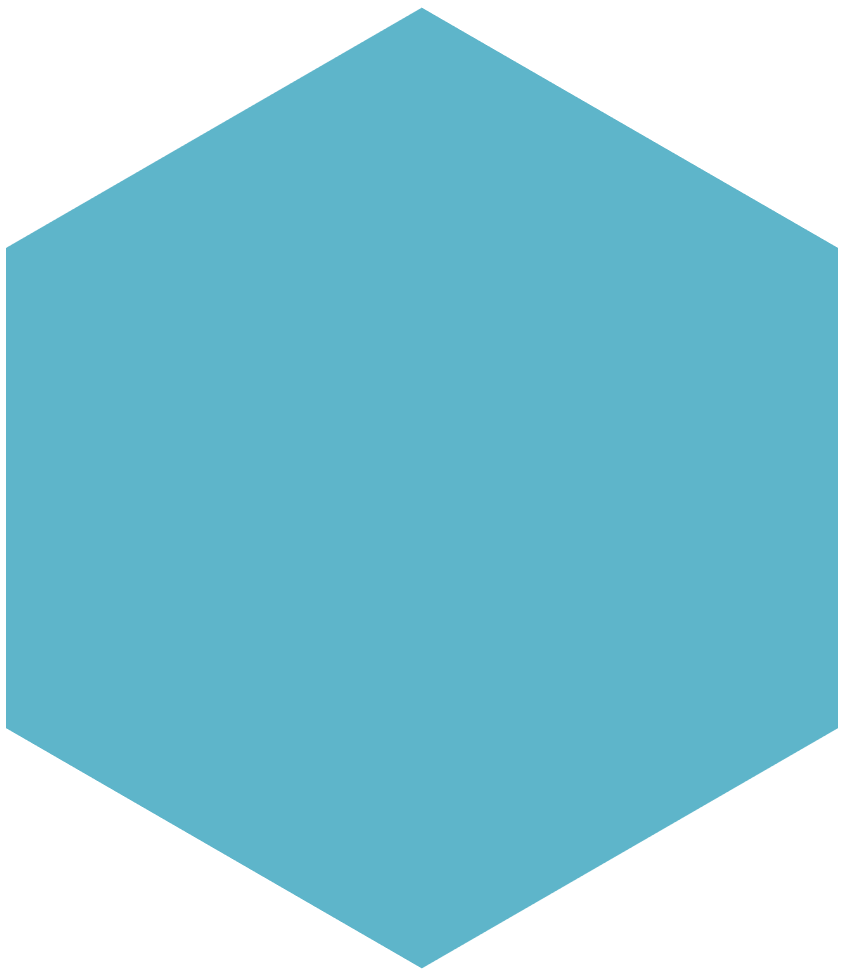


Digital HaïTian Gourde



CAHIER DES CHARGES

2019-2020

Auteurs :

Thomas BEATINI  
Arnaud FERNANDEZ  
Chloé MACCARINELLI  
Cédric ORTEGA

Tuteurs :

Gabriel MOPOLO-MOKE

Alexandre MAISONOBE

Gaëtan LESCOUFLAIR

# Table des matières

[I. Introduction](#_Toc33455467)

[II. Cas d’utilisation particuliers et commerçants](#_Toc33455468)

[II.1 Cas numéro 1](#_Toc33455469)

[II.2 Cas numéro 2](#_Toc33455470)

[II.3 Cas numéro 3](#_Toc33455471)

[II.3.1 Cas numéro 3.1](#_Toc33455472)

[II.3.2 Cas numéro 3.2](#_Toc33455473)

[II.3.3 Cas numéro 3.3](#_Toc33455474)

[III. Cas d’utilisation institutions financières](#_Toc33455475)

[IV. Cas d’utilisation BRH](#_Toc33455476)

[V. Spécifications et contraintes](#_Toc33455477)

[les règles suivantes doivent être respectées](#_Toc33455478)

[VI. Architecture logicielle](#_Toc33455479)

[Détails de l’architecture](#_Toc33455480)

[VII. Base de données MySQL](#_Toc33455481)

[Description des tables](#_Toc33455482)

[VIII. Conception des interfaces web et mobile](#_Toc33455483)

[IX. Calendrier prévisionnel](#_Toc33455484)

[X. Plan des risques](#_Toc33455485)

# Introduction

La monnaie nationale d’Haïti, la gourde (HTG), de nature très volatile et en dépréciation continue depuis les vingt dernières années, le gouvernement Haïtien en collaboration avec la Banque de la République d’Haïti (BRH) cherchent une solution pour relancer l’économie du pays.

La solution proposée par le projet Digital Gourde (DHTG), est la mise en place d’une cryptomonnaie d’état du même nom qui sera gérée, supervisée et distribuée par la BRH et mis à disposition des institutions financières locales.

Les objectifs à long terme du projet sont de :

* Réduire puis supprimer le coût de fabrique et d’importation de la monnaie physique
* Permettre aux personnes non-bancarisées d’Haïti de l’être, sans risques pour les institutions financières
* Augmenter le taux de change de la monnaie nationale pour combler le déficit financier du pays

L’avantage majeur de l’utilisation des cryptomonnaies dans un cas tel que celui-ci est que la création de la monnaie est instantanée et sans frais. Aussi, chaque opération utilisant cette monnaie (distribution, paiement, virement, etc.) aura un coût extrêmement faible et sera instantanée étant donné que la blockchain sur laquelle elle se base utilise une architecture client-serveur plutôt qu’un système de Proof of Work, contrairement aux cryptomonnaies tels que le Bitcoin.

La réalisation du projet se base sur la distinction entre 4 profils :

La banque centrale : Cet acteur représente la BRH, c’est elle qui va accorder les habilitations aux institutions financières et surveiller ce réseau

Les institutions financières : Ce sont toutes les banques Haïtiennes (Sogebank, Citibank, etc…) qui vont gérer les opérations des particuliers et commerçants sur le réseau

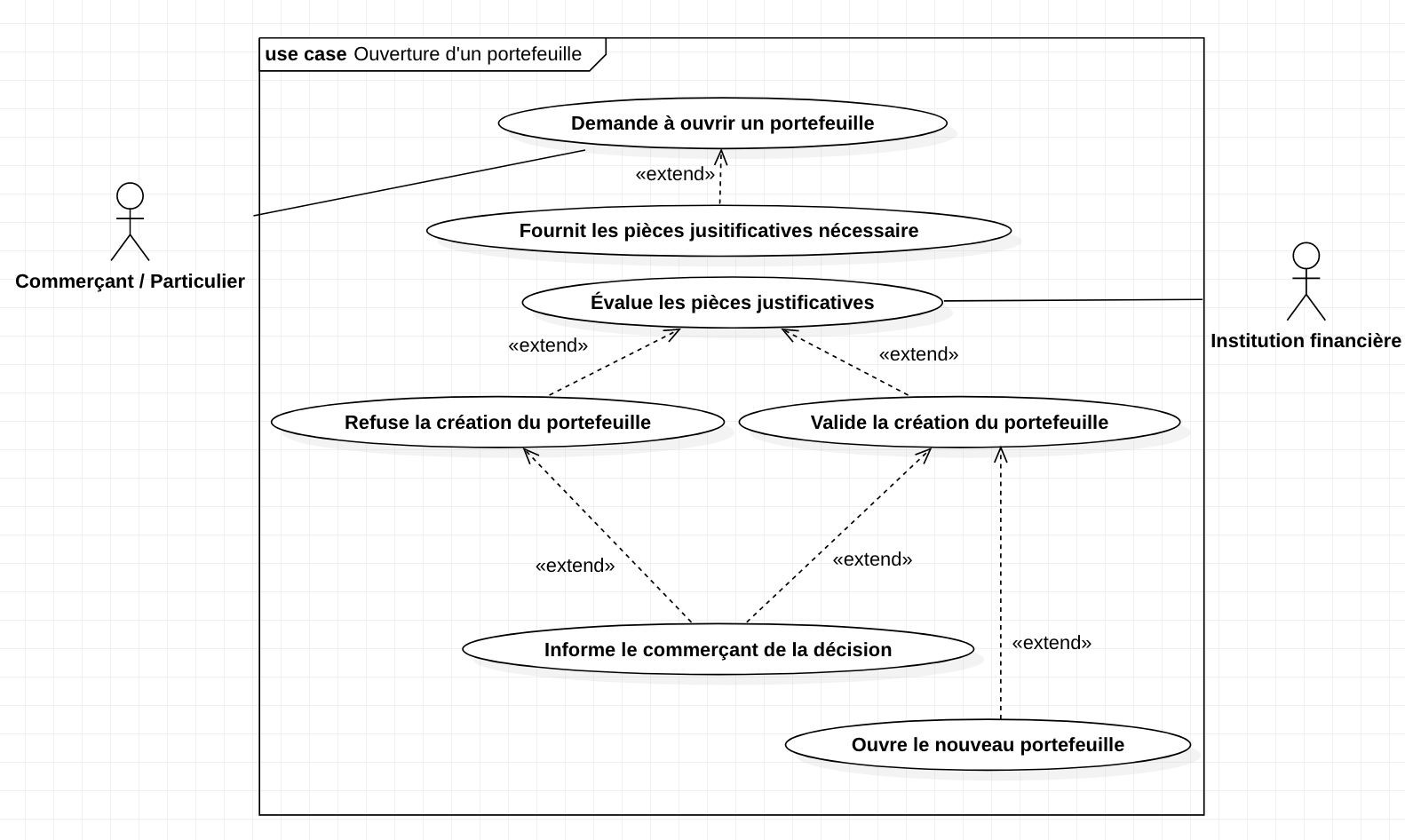
Les particuliers : Les personnes qui souhaitent accéder aux services qu’offrent les institutions financières dans un contexte personnel, c’est-à-dire pour effectuer des paiements chez des commerçants, faire des virements.

Les commerçants : Ces acteurs sont une variation des particuliers destinée aux professionnels souhaitant mettre à disposition des moyens de paiement à leurs clients

# Cas d’utilisation particuliers et commerçants

## II.1 Cas numéro 1

Un commerçant/particulier doit pouvoir demander l’ouverture d’un portefeuille à une institution financière en fournissant ses informations personnelles et pièces justificatives depuis l’application web ou mobile.



**Description détaillée**

Figure 1 : Use Case ouverture de portefeuille

**Résumé :**

Ce CU décrit le passage d'une commande par un Client web, depuis la connexion au site jusqu'à l'envoi du mail de confirmation de commande.

**Acteurs :** Client Web(particuliers/commerçants) ou Administrateurs

**Précondition :** Pas de précondition

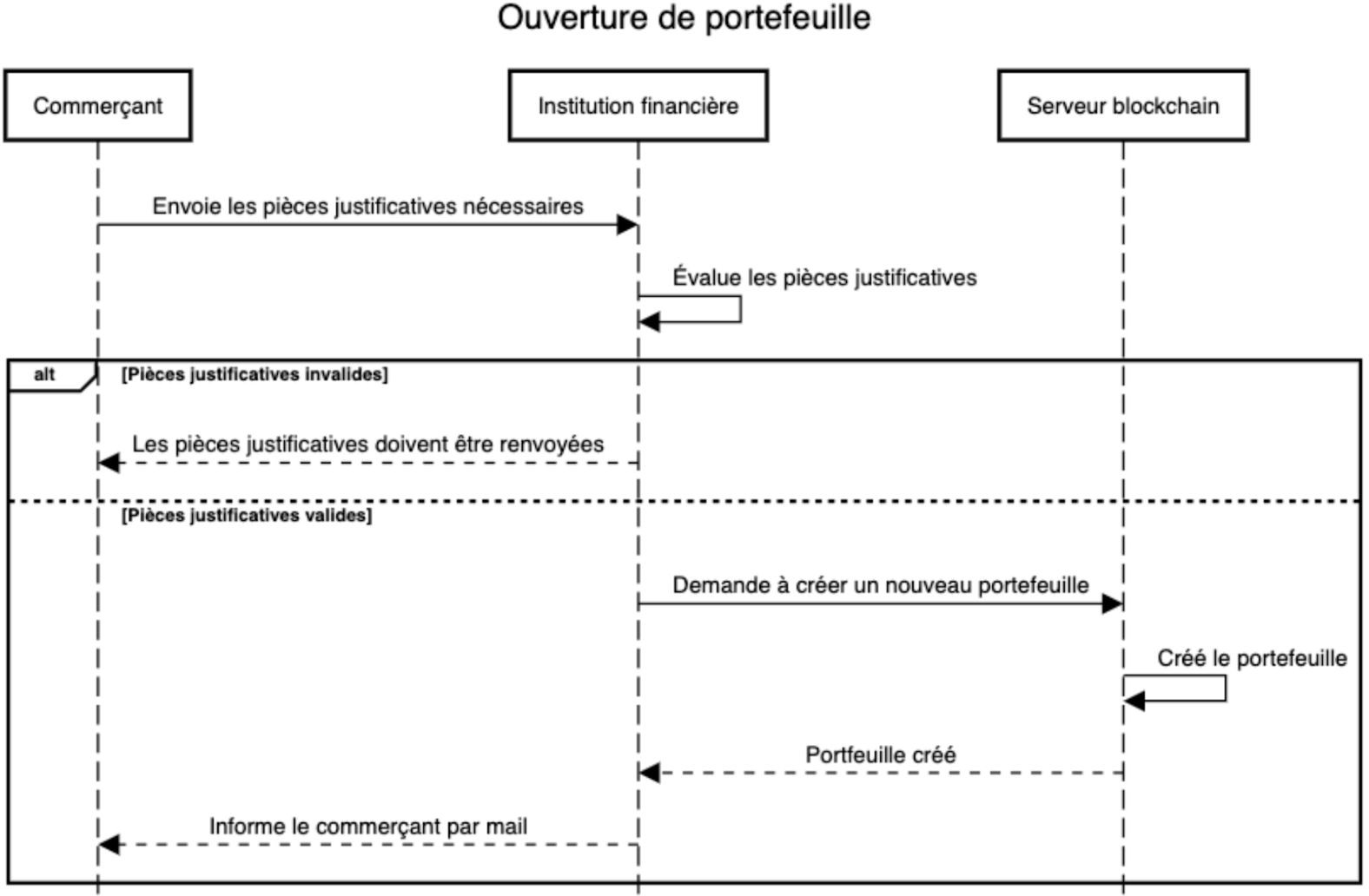
**Post condition :** Un nouveau portefeuille est créé avec une adresse pouvant effectuer des transactions

**Déroulement normal :**

Le CU commence quand le client veut se connecter au système et qu’il n’a pas encore de portefeuille. Il lui est demandé de créer un nouveau portefeuille. En créant son nouveau portefeuille, des documents doivent être remis. Ces documents seront validés ou non par les administrateurs de la Banque concernée. Les documents validés vont permettre la création du portefeuille et le client sera informé par mail que celui-ci est bien créé.

**Le cas d'utilisation est terminé**

Figure 2 : Diagramme de séquence Ouverture de portefeuille



## II.2 Cas numéro 2

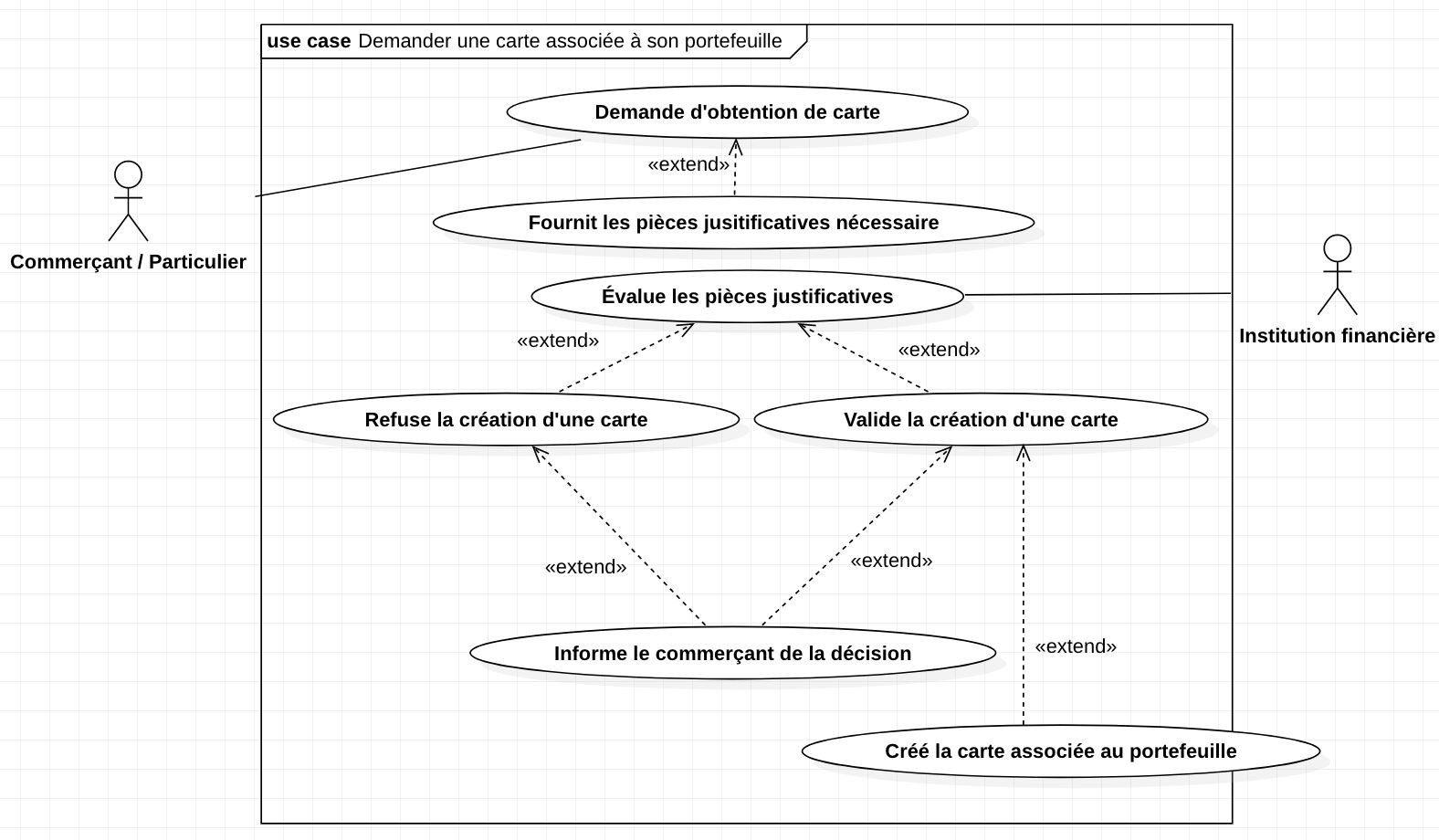
Un commerçant/particulier doit pouvoir demander une carte associée à l’un de ses portefeuilles à l’institution financière qui le gère depuis l’application web ou mobile.   


Figure 3 : Use case demande de carte

**Description détaillée**

**Résumé :**

Ce CU décrit le passage d'une commande de carte par un Client web, depuis la connexion au site jusqu'à l'envoi de la carte.

**Acteurs :** Client Web(particuliers/commerçants) ou Administrateurs

**Précondition :** Avoir un portefeuille actif

**Post condition :** Une nouvelle carte pouvant effectuer des paiements et retraits

**Déroulement normal :**

Le CU commence quand le client veut demander une carte rattachée à son portefeuille. La carte est créée et rattachée au portefeuille du client. La carte est envoyée au client.

**Le cas d'utilisation est terminé**

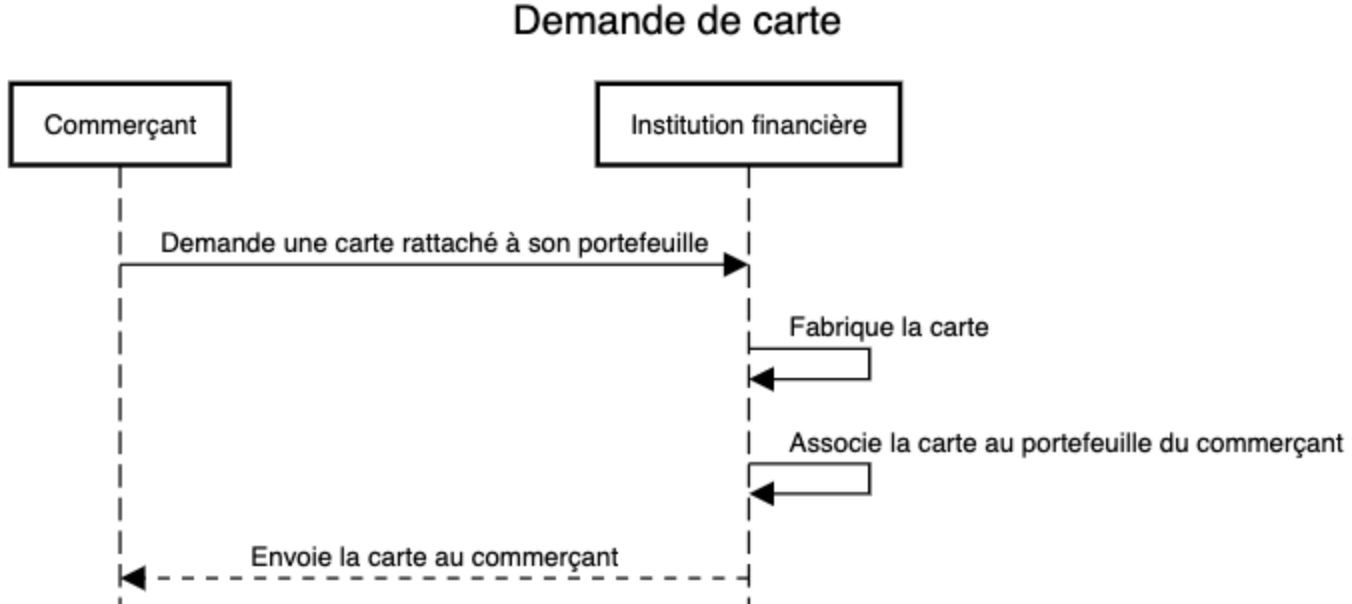


Figure 4 : Diagramme de séquence demande de carte

## II.3 Cas numéro 3

Un commerçant/particulier doit pouvoir gérer ses portefeuilles (relevés du portefeuille, consultation du solde, virement vers un autre portefeuille via NFC, QR code ou par saisie manuelle) depuis l’application web ou mobile, et effectuer des dépôts ou retraits gourdes physiques avec ces derniers.

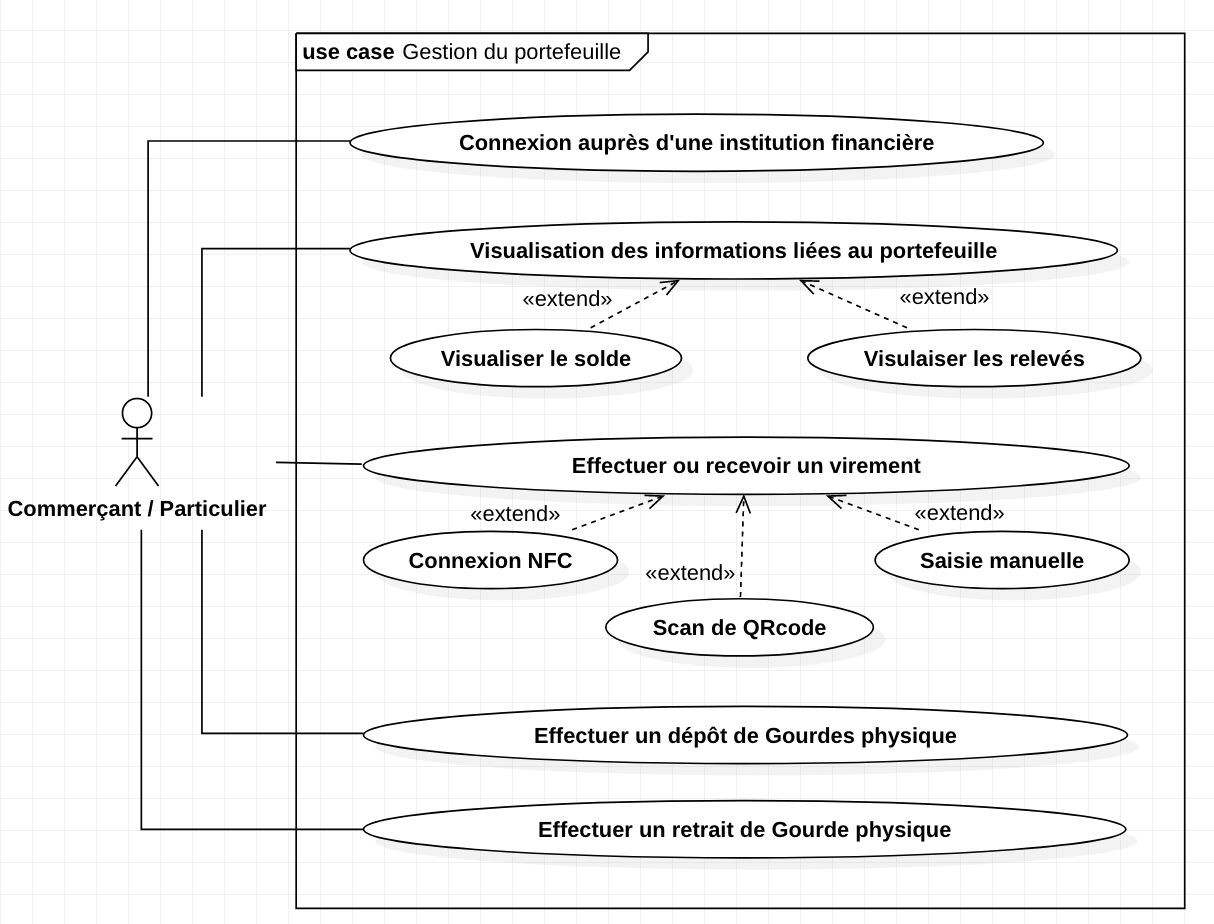


Figure 5 : Use case gestion du portefeuille

### II.3.1 Cas numéro 3.1

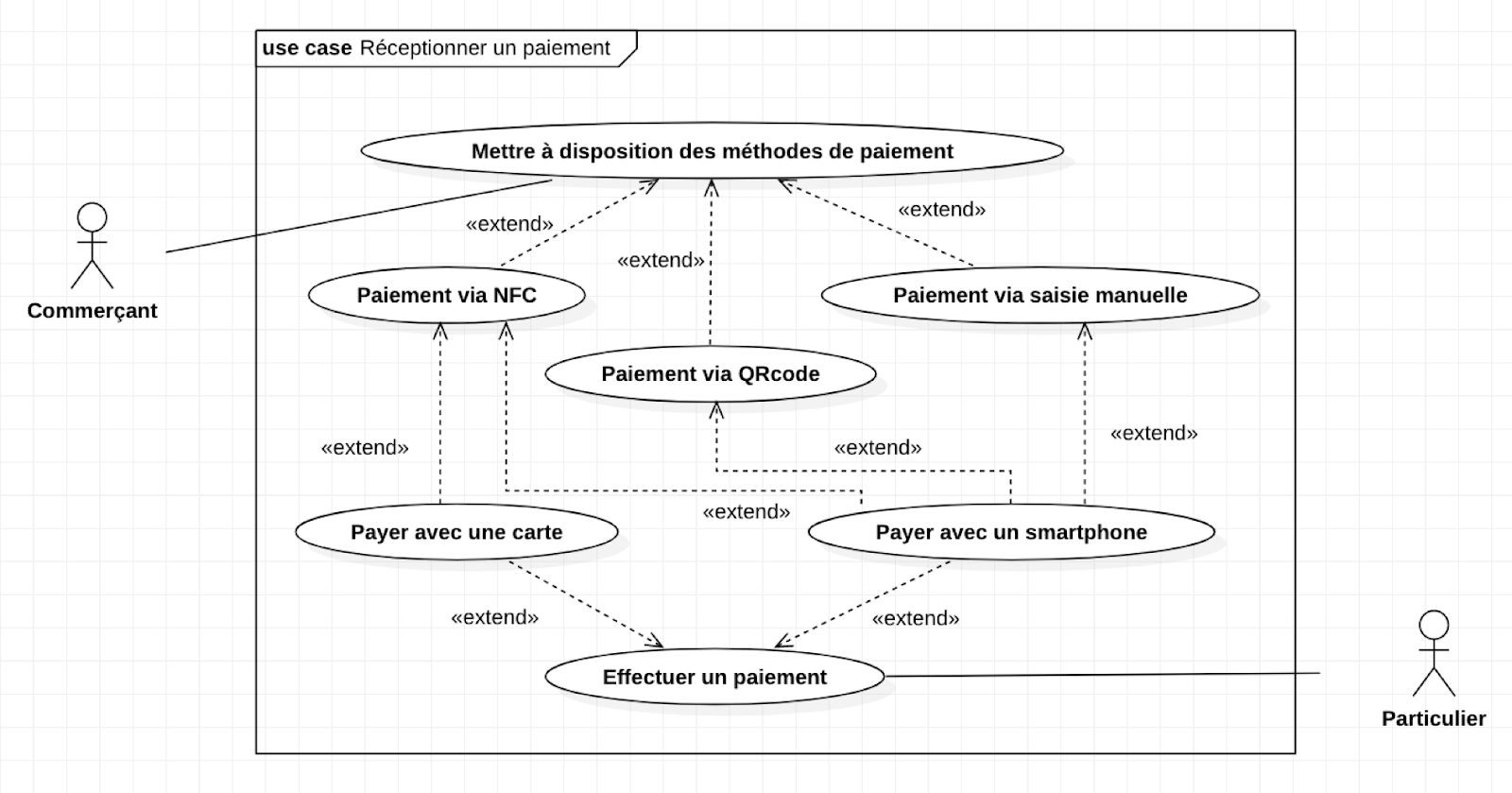
Un commerçant doit pouvoir réceptionner des paiements en DHTG venant d’une carte ou d’un mobile, le particulier doit pouvoir les effectuer.

Figure 6 : Use case réception de paiement

**Description détaillée**

**Résumé :**

Ce CU décrit la réception de paiement en DHTG d’un commerçant via carte ou smartphone.

**Acteurs :** Client Web(particuliers/commerçants) ou Administrateurs

**Précondition :** Avoir un portefeuille actif

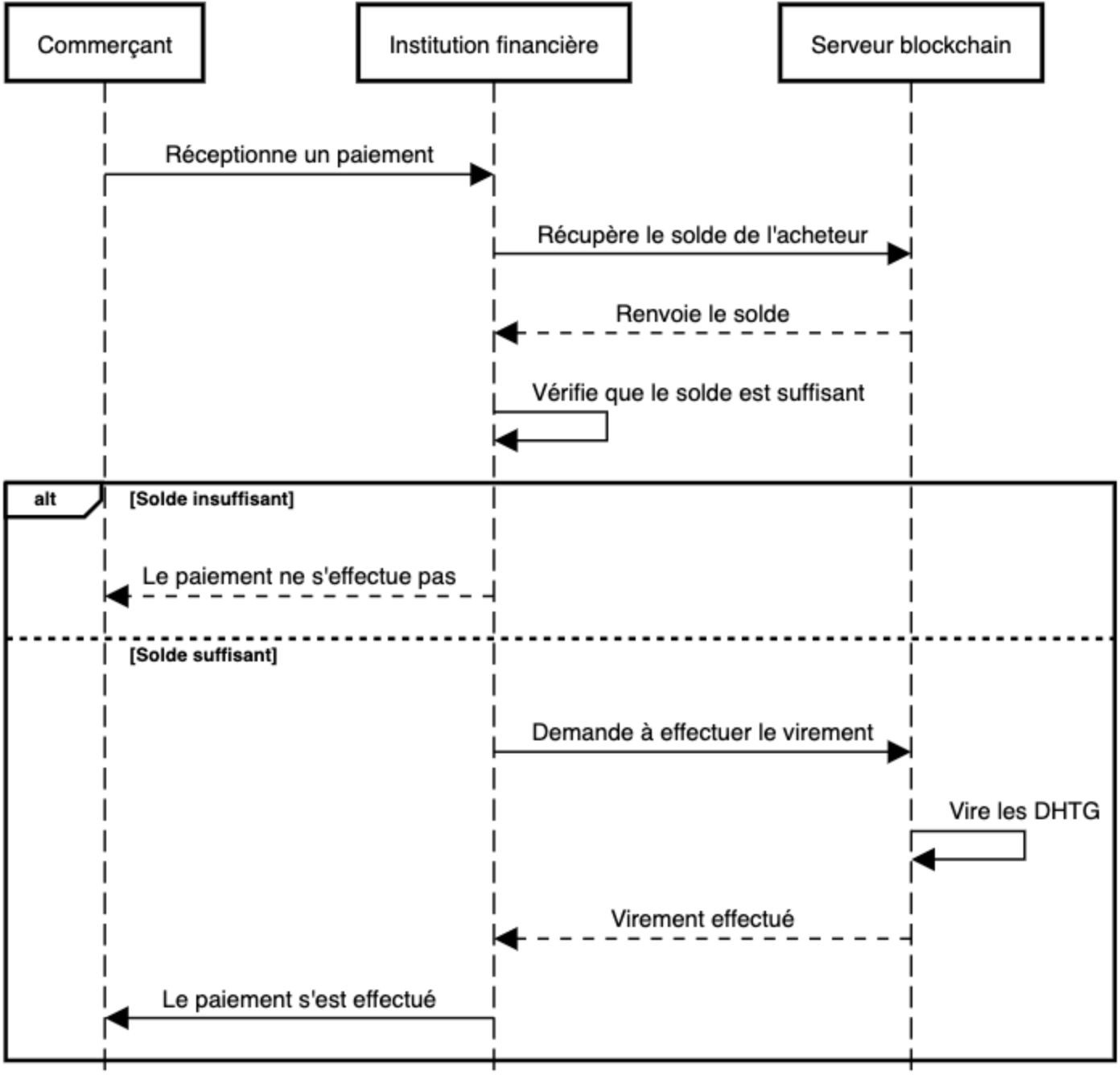
**Post condition :** Un crédit correspondant au paiement

**Déroulement normal :**

Le paiement est réceptionné, le solde de l’acheteur est évalué. S’il est suffisant le paiement est effectué sinon refusé.

**Le cas d'utilisation est terminé**

Figure 7 : Diagramme de séquence réception de paiement



### II.3.2 Cas numéro 3.2

Un commerçant doit pouvoir réceptionner un dépôt de gourdes physiques et transférer les fonds en DHTG vers la personne les ayant déposées en lisant le numéro du portefeuille concerné via mobile ou carte (NFC et QRcode), un particulier doit pouvoir les déposer.

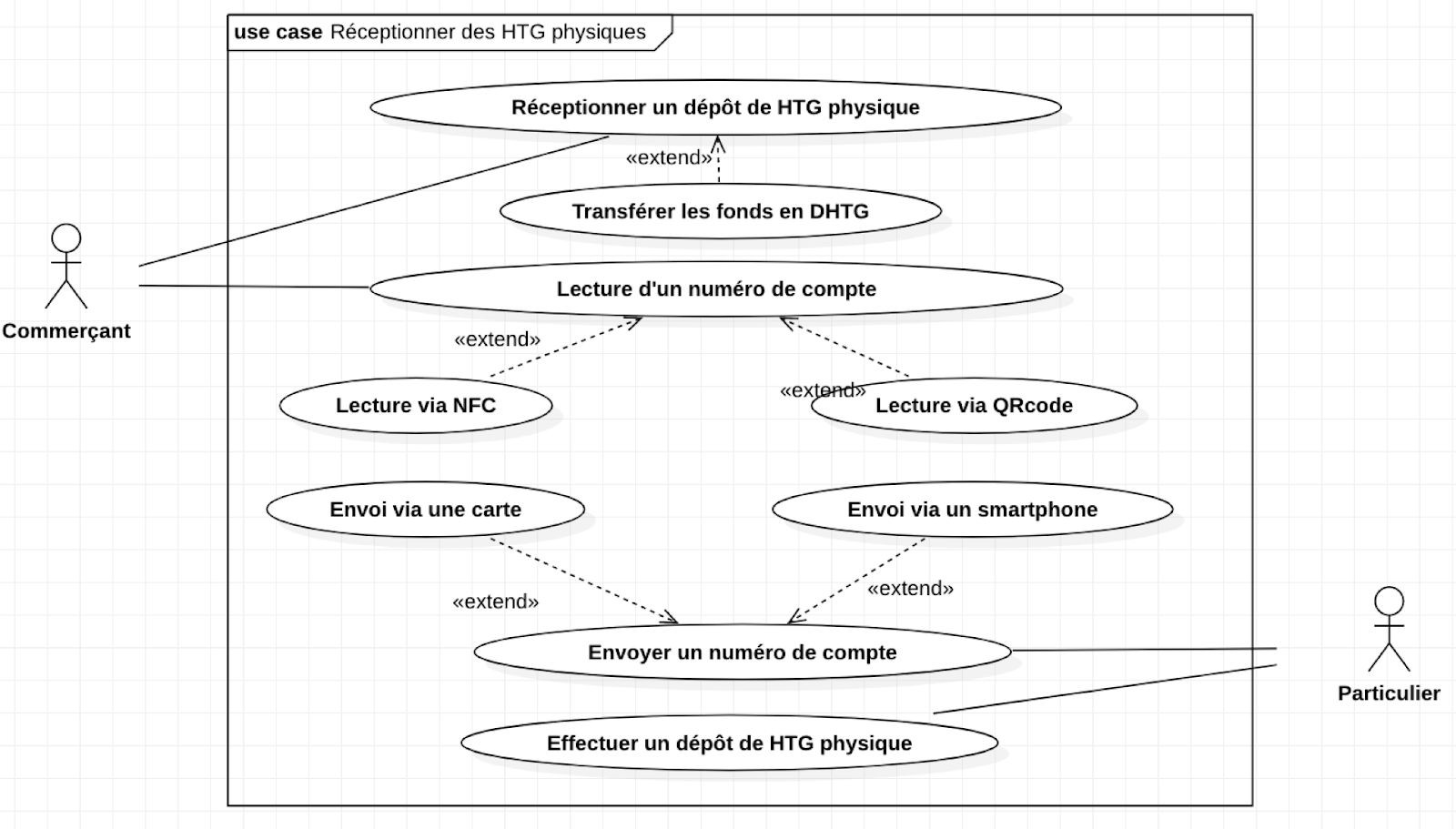


Figure 8 : Use case réception DHTG

**Description détaillée**

**Résumé :**

Ce CU décrit la réception de DHTG physique d’un commerçant.

**Acteurs :** Client Web(particuliers/commerçants) ou Administrateurs

**Précondition :** Avoir un portefeuille actif

**Post condition :** Un crédit physique correspondant au dépôt et un débit de DHTG correspondant au dépôt (pour le commerçant) et inversement pour le particulier

**Déroulement normal :**

Le commerçant récupère le dépôt de DHTG physique. Le commerçant effectue un virement correspondant au montant vers le déposeur. Le solde du commerçant est analysé. Si son solde est suffisant le virement est effectué sinon refusé.

**Le cas d'utilisation est terminé**

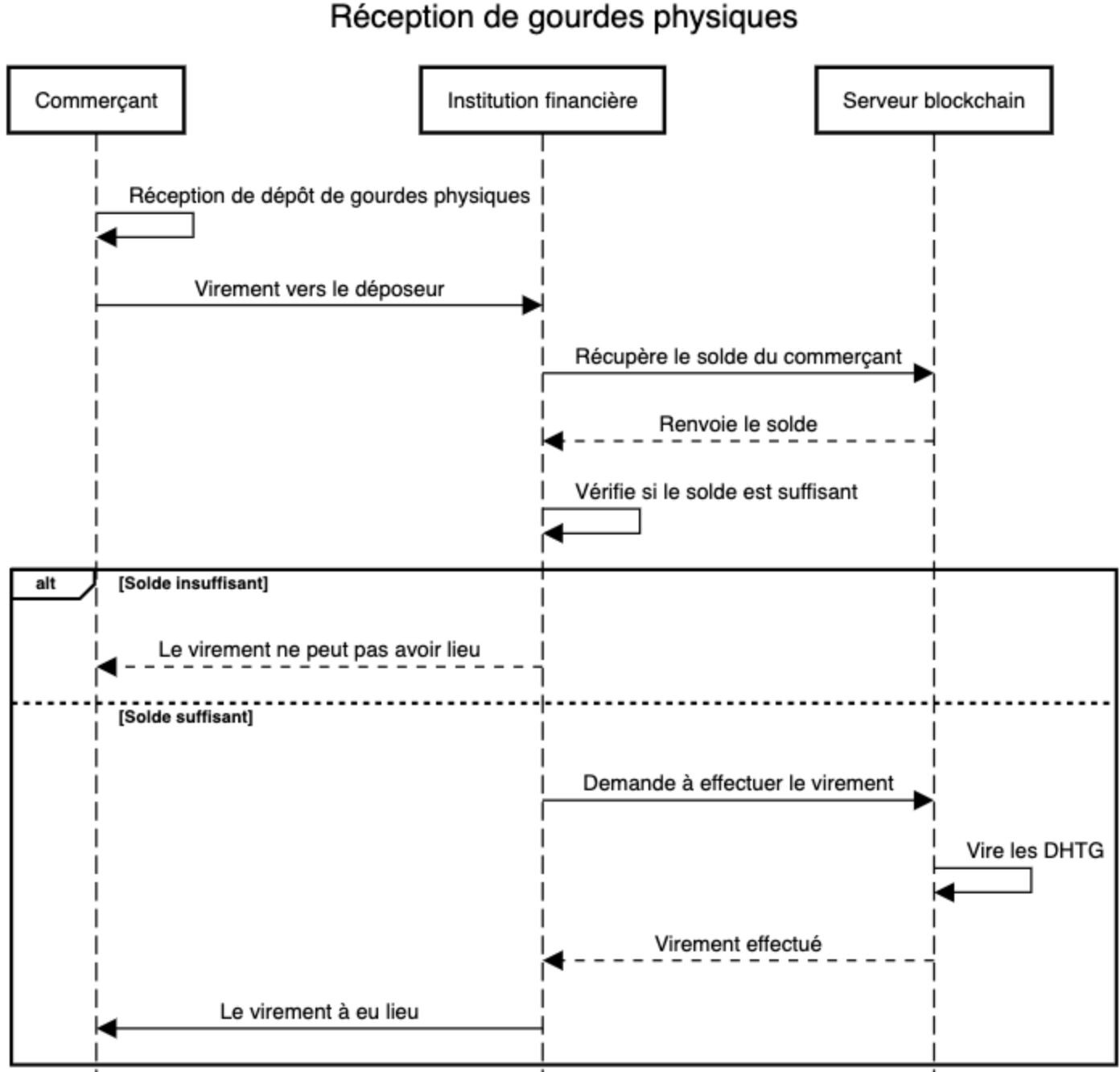


Figure 9 : Diagramme de séquence réception DHTG

### II.3.3 Cas numéro 3.3

Un commerçant doit également être en mesure d’effectuer tout autre activité auquel ont accès les particuliers, tels que le paiement chez d’autres commerçants via carte, mobile ou saisie manuelle du numéro de portefeuille ou bien le dépôt de gourdes physiques chez d’autres commerçants.

**(cf Cas détaillés ci-dessus)**

# Cas d’utilisation institutions financières

1. cas d’utilisation similaires à ceux des particuliers

* Demander une habilitation à la banque centrale (attention justificatifs) depuis le site web de la banque centrale
* Demander l’ouverture d’un portefeuille à la banque centrale (attention justificatifs) depuis le site web de la banque centrale
* Gérer son portefeuille (relevés du portefeuille, solde, transfert portefeuille à portefeuille (via NFC, QR Code, saisie manuelle), transférer de son compte en gourdes physiques à la banque centrale un montant vers son portefeuille à la banque centrale)

1. cas d’utilisation spécifiques aux institutions financières

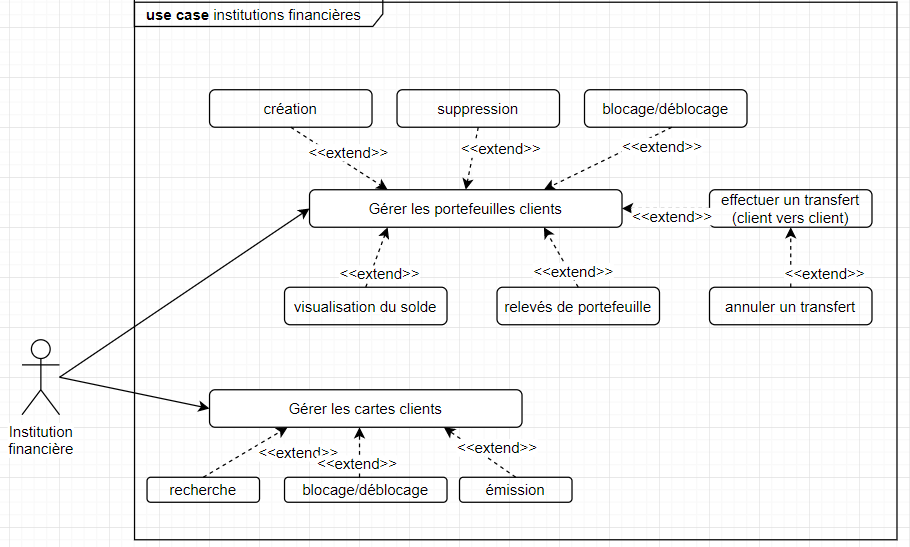
* Gérer les portefeuilles clients (particuliers ou commerçants) (création, modification, suppression, restaurer, bloquer/débloquer, validation, édition de relevés de transactions)
* Gestion des cartes clients (émission, blocage, déblocage, recherche, …)

Figure 10 : Use case institutions financières

# Cas d’utilisation BRH

* La BRH doit avoir une vue sur tout le réseau (institutions financières, commerçants, particuliers) et donc pouvoir réaliser les mêmes actions.

# Spécifications et contraintes

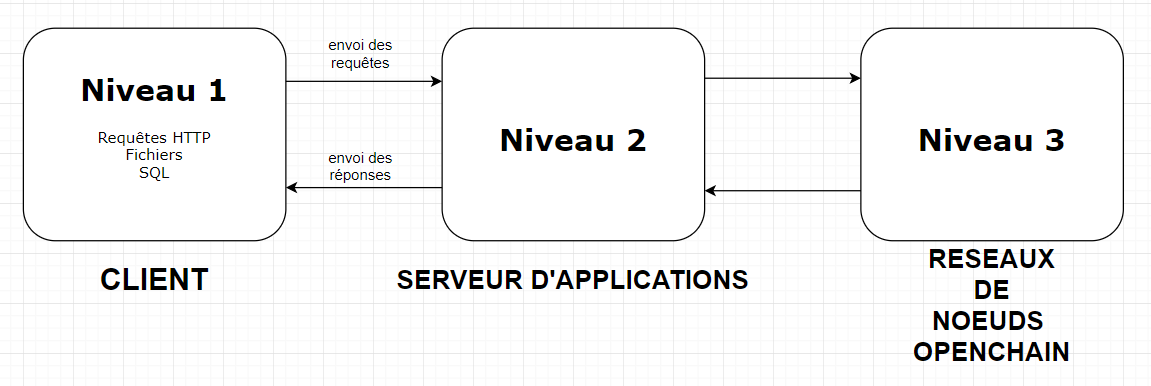
L’application doit être scalable et facilement utilisable par tout utilisateur, elle doit donc répondre à certaines spécifications.

De plus, certaines règles de logiques doivent être introduites dans le processus de développement pour respecter le fonctionnement classique d’une banque.

## les règles suivantes doivent être respectées

* Nous supposons que le propriétaire de l’application est la banque centrale d’Haïti (BRH)
* Toutes les opérations doivent faire l’objet de vérifications
* Le solde d’un portefeuille ne peut être négatif :
  1. La banque centrale ne peut distribuer aux institutions financières plus que le montant restant émis en gourde électronique disponible dans son portefeuille
  2. Une institution financière ne peut distribuer à ses clients plus que ce qu’elle possède dans son portefeuille
  3. Un particulier ou commerçant ne peut virer ou retirer plus que ce qu’elle possède dans son portefeuille
* La banque centrale peut à tout moment faire une nouvelle émission de monnaies électroniques
* Quel que soit l’opération, on débite toujours un portefeuille pour créditer un autre portefeuille
* Un portefeuille est toujours rattaché à une banque

# Architecture logicielle



## Détails de l’architecture

I/ Clients web et mobile par lesquels nos divers profils pourront accéder aux services de DHTG. La connexion à ceux-ci peut être soit via le web, soit via une application mobile, c’est ici que les demandes d’opérations seront effectuées.

II/ Les clients web et mobile communiquent avec une API REST (node js) qui fait le lien entre la blockchain OpenChain (transactions, portefeuilles, cryptomonnaie), les données des banques et des utilisateurs (stockées dans une base de données MySQL) et les clients web et mobile

III/ Finalement, l’instance OpenChain qui gère les transactions de la blockchain est hébergée dans un conteneur Docker avec un base de données MongoDB où seront stocker les données liées aux transactions

Pour s’assurer de la **sécurité** des données du système, tous les mots de passe dans la base de données seront cryptés et l’API REST sera accessible qu’en HTTPS pour en garantir la fiabilité.

Dans un souci de **robustesse**, on limitera le nombre de requêtes vers l’API à 100 toutes les 15 minutes par adresse IP afin d’éviter les attaques DDOS.

# Base de données MySQL

Figure 11 : Visualisation de la BDD MySQL

La base des données MySQL est utilisée pour gérer les informations relatives aux utilisateurs. Dans le cadre du projet cette base des données est déployée par la BRH qui a le contrôle absolu sur les données

## Description des tables

**Utilisateur :** représente tout compte permettant de se connecter à l’application

**Banque :** représente la banque de rattachement d’un utilisateur

**Role :** représente le niveau de permissions de l’utilisateur, plus il est élevé, plus il aura accès à des fonctionnalités dans l’API

**Document :** représente les documents qu’un utilisateur a envoyé pour valider l’ouverture de son premier portefeuille

**Status :** représente le statut de validation (ou non) des documents envoyés par l’utilisateur

**TokenVerification :** permet l’activation d’un compte après envoi du mail de création

**Portefeuille :** représente tous les numéros de portefeuille détenus par un utilisateur, la base de données ne gère pas les portefeuilles d’Openchain

**Carte :** représente toutes les cartes rattachées à un portefeuille

**Beneficiaire :** représente toutes les personnes à qui un utilisateur peut faire des virements

**Motiftransaction :** représente le motif correspondant à une transaction

# Conception des interfaces web et mobile

Le développement des interfaces mobiles n’a pas été pris en compte à ce stade du projet. Les interfaces web quant à elles nécessitent un rafraîchissement.

L’utilisation d’un Framework tel que Flutter va nous permettre de mettre en place qu’une seule phase de développement. En effet, un tel Framework tout support permettra de déployer aussi bien l’application sur Web, Android ou IOS avec une seule implémentation.

Une telle solution comporte plusieurs avantages :

* Tout d’abord, l’application serait multiplateforme, tout utilisateur de smartphone serait capable de l’utiliser (Android, iOS ou autre)
* Le développement serait simplifié, l’application sera recentrée sur un même projet de développement comportant des composants web et mobile plutôt que d’avoir une application native pour chaque système d’opération bien plus coûteux et complexe à maintenir/évoluer
* Si l’utilisateur mobile souhaite installer l’application sur son appareil, il pourra bénéficier de fonctionnalités qui ne seraient habituellement pas accessibles depuis une plateforme web, notamment l’usage de la NFC, de la caméra (lecture de QR code).

# Calendrier prévisionnel

|  |  |
| --- | --- |
| Élaboration du cahier des charges  Etat de l’art  Prise en main du projet  Mise en place de l’environnement et nouvelle technologie (Flutter) | 15/11/2019 au  01/02/2020 |
| Recherche de faille de sécurité, amélioration et implémentation du niveau de sécurité de certaines fonctionnalités | 01/02/2020 au 20/02/2020 |
| Amélioration de la partie client web et implémentation du client mobile | 20/02/2020 au 20/03/2020 |
| Documentation, test et déploiement de l’application | 20/03/2020 au  30/03/2020 |

La nature prévisionnelle de ce calendrier pourrait cependant l’amener à être modifié au niveau des dates estimées, elles restent donc plus ou moins flexibles.

Avec une estimation de travail de 18 Jours Homme par mois sur 5 mois, on estime le coût du projet à 18JH \* 5 mois = 90JH.

# Plan des risques

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Libellés | Priorité | Facteurs | Actions | Statut / date début du risque | Coût |
| Ne plus disposer de la maintenance de l’outil Open Source (Openchain) | 3 | Maintenance annulée par les contributeurs | -Formation sur un nouvel outil et implémentation  -Consultant pour le changement d’outils  (Prévoir un budget supplémentaire) | Plus tard | 20 JH  Ou \*\* |
| Ne pas pouvoir réaliser le prototype à temps | 5 | -Cahier des charges non définies  -Le temps impartie pour la réalisation du projet | -Implémenter les cas d’utilisation les plus important  -Délai supplémentaire | En cours /  20/02/2020 | 20JH |