

Digital HaïTian Gourde

MASTER 2 MIAGE MBDS

2019-2020

Auteurs :

Thomas BEATINI
Arnaud FERNANDEZ
Chloé MACCARINELLI
Cédric ORTEGA

Tuteurs :

Gabriel MOPOLO-MOKE
Alexandre MAISONOBE
Gaëtan LESCOUFLAIR



MIAGE
RÉSEAU
DES MIAGE
DE FRANCE
Nice

UNIVERSITÉ
CÔTE D'AZUR

MBDS

BRI

BANQUE DE LA RÉPUBLIQUE D'HAÏTI



Table des matières

I.	Liste des figures.....	3
II.	Résumé	4
III.	Abstract.....	4
IV.	Introduction	5
V.	Présentation des acteurs	6
	V.1 Présentation de l'Université Côte d'Azur (MBDS)	6
	V.1.1 Mobilité, Base de Données/Big Data et Intégration de Systèmes (MBDS).....	6
	V.2 Présentation de la BRH (Banque de la République d'Haïti)	6
VI.	Etat de l'art.....	7
	VI.1. La blockchain	7
	VI.1.1. Définition	7
	VI.1.2 Les règles de consensus.....	7
	VI.2 Les types de blockchains	8
	VI.2.1 PUBLIQUE	8
	VI.2.2 PRIVE ("DISTRIBUTED LEDGER TECHNOLOGY" (DLT))	8
	VI.2.3 Critères relatifs à notre projet.....	10
	VI.3 La crypto-monnaie	10
	VI.3.1 Définition	10
	VI.3.2 Les différentes crypto-monnaies.....	11
	VI.3.3 Critères relatifs à notre projet.....	11
VII.	Etude de l'existant	12
	VII.1 L'environnement	12
	VII.1.1 Openchain.....	12
	VII.1.2 Hyperledger Fabric, une alternative à Openchain	13
	VII.1.3 MySQL – API REST NodeJs – Angular 7	15
VIII.	Démarche projet	16
	VIII.1 Gestion de projet	16
	VIII.2 Contraintes, outils et risques.....	16
	VIII.2.1 Contraintes	16
	VIII.2.2 Outils	17
	VIII.2.3 Risques	17
	VIII.3 Planning	18
	VIII.4 Budget.....	19
IX.	Exigences fonctionnelles.....	19
	IX.1 Les acteurs de niveau fonctionnel	19

IX.2 Les cas d'utilisation.....	20
IX.2.1 Cas d'utilisation particuliers et commerçants (Partie Web)	20
IX.2.2 Cas d'utilisation particuliers et commerçants (Partie Mobile)	35
IX.2.3 Cas d'utilisation institutions financières.....	36
IX.2.4 Cas d'utilisation BRH.....	39
X. Exigences non-fonctionnelles	42
X.1 Utilisabilité	42
X.2 Performances	42
X.3 Robustesse	42
X.4 Sécurité	42
X.5 Maintenabilité, évolutivité.....	42
XI. Architectures	43
XI.1 Niveau 1	43
XI.2 Niveau 2	44
XI.3 Niveau 3	45
XII. Les Améliorations	46
XII.1 Client Web	46
XII.2 Client mobile	46
XIII. Déploiement.....	47
XIV. Perspectives.....	48
XIV.2 Client Web et mobile	48
XIV.2.1 Framework Flutter.....	48
XIV.2.2 Langage Dart.....	48
XV. Conclusion	49
XVI. Webographie et Bibliographie.....	50

I. Liste des figures

<i>Figure 1 : Fonctionnement d'une blockchain</i>	7
<i>Figure 2 : Les différentes règles de consensus (La Blockchain- Panorama des technologies existantes © 2017 Deloitte SAS).....</i>	8
<i>Figure 3 : Différences entre blockchain privée et publique (La Blockchain- Panorama des technologies existantes © 2017 Deloitte SAS).....</i>	9
<i>Figure 4 : Qu'est-ce que la crypto-monnaie ?</i>	10
<i>Figure 5: Des possibilités technologiques révolutionnaires.....</i>	11
<i>Figure 6 : Schématisation d'un bloc caché.....</i>	14
<i>Figure 7 : Architecture Hyperledger Fabric.....</i>	14
<i>Figure 8 : Fonctionnement PoC</i>	15
<i>Figure 9 : Kanban DigitalGourde</i>	16
<i>Figure 10 : Diagramme de Gantt.....</i>	18
<i>Figure 11 : Estimation du nombre de jours de travail</i>	18
<i>Figure 12 : Estimation du coût du projet.....</i>	19
<i>Figure 13 : Les acteurs.....</i>	19
<i>Figure 14 : Use Case authentification</i>	20
<i>Figure 15: Diagramme de séquence authentification.....</i>	21
<i>Figure 16 : Use Case ouverture de portefeuille</i>	23
<i>Figure 17 : Diagramme de séquence Ouverture de portefeuille</i>	24
<i>Figure 18 : Use case demande de carte</i>	26
<i>Figure 19 : Diagramme de séquence demande de carte.....</i>	27
<i>Figure 20 : Use case gestion du portefeuille.....</i>	28
<i>Figure 21 : Use case réception de paiement</i>	29
<i>Figure 22 : Diagramme de séquence réception de paiement.....</i>	30
<i>Figure 23 : Use case réception DHTG.....</i>	32
<i>Figure 24 : Diagramme de séquence réception DHTG</i>	33
<i>Figure 25: Diagramme de séquence effectuer un virement</i>	34
<i>Figure 26 : Diagramme de séquence visualiser son relevé.....</i>	35
<i>Figure 27 : Use case institutions financières.....</i>	37
<i>Figure 28 : Diagramme de séquence demande d'habilitation</i>	39
<i>Figure 29 : Architecture générale de l'application</i>	43
<i>Figure 30 : Architecture technique générale de l'application</i>	43
<i>Figure 31: Architecture client</i>	44
<i>Figure 32: Architecture serveur</i>	44
<i>Figure 33 : Architecture Docker Openchain</i>	45
<i>Figure 34 : Architecture complète</i>	46
<i>Figure 35 : Déploiement</i>	47

II. Résumé

Ce projet consiste à la réalisation d'une cryptomonnaie sociale, monnaie virtuelle d'échange, sécurisée permettant de faciliter et révolutionner le paiement et les transferts d'argent.

Il prend principalement en compte ceux qui sont non bancarisés de la population Haïtienne. Cette monnaie pourrait être utilisée dans plusieurs domaines tels que l'agriculture, l'éducation, la santé, etc.

Une technologie appelée blockchain, qui par ses propriétés intrinsèques, apporte une facilité et rapidité des échanges. Cette technologie sera la base de notre moyen d'échange, car elle offre un environnement de confiance.

En effet la blockchain est une base de données répliquée, décentralisée donc il n'y pas une autorité centrale. Une fois une transaction validée, il est impossible de l'effacer et toute tentative de falsification est rendue extrêmement complexe. De plus, il y a l'anonymat des utilisateurs réalisé par la cryptographie.

La blockchain créée sera privée, car les transactions seront vérifiées et validées par ceux qui sont autorisés à se connecter sur la blockchain. Cela permet une plus grande efficacité, évolutivité, une faible consommation énergétique. De plus les transactions sur une blockchain privée sont validées beaucoup plus rapidement.

III. Abstract

This project consists of the creation of a social cryptocurrency; virtual exchange currency, secure to facilitate and revolutionize the payment and the transfer of money. It mainly considers those who are unbanked of the Haitian population. This currency could be used in several sectors such as agriculture, education, health, etc.

A technology called blockchain which, by its intrinsic properties, brings a facility and rapidity of the exchanges, security of the transactions and an environment of confidence, will be the base of our medium of exchange.

Indeed, the blockchain is a replicated database, decentralized so there is no central authority. Once a transaction is validated, it cannot be erased and any attempt to falsify is rendered extremely complex. In addition, there is the anonymity of the users realized by the cryptography.

The created blockchain will be private because the transactions will be verified and validated by those who can connect to the blockchain. This allows for greater efficiency, scalability, low energy consumption. In addition, transactions on a private blockchain are validated much more quickly.

IV. 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 :

1. Réduire puis supprimer le coût de fabrique et d'importation de la monnaie physique
2. Permettre aux personnes non-bancarisées d'Haïti de l'être, sans risques pour les institutions financières
3. 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.

V. Présentation des acteurs

V.1 Présentation de l'Université Côte d'Azur (MBDS)

L'université Nice Côte d'Azur est une université française pluridisciplinaire. L'université est implantée à Nice et dans le département des Alpes-Maritimes.

V.1.1 Mobilité, Base de Données/Big Data et Intégration de Systèmes (MBDS)

La spécialité MBDS est la proposition d'une restructuration et d'intégration de cette spécialité au sein de la mention MIAGE de Nice. En effet, l'informatique d'entreprise mise en avant par MIAGE est le thème principal naturel de cette spécialité. Dans l'intégration de cette spécialité à la mention MIAGE, nous avons complété la partie très technique du MBDS historique par la double compétence en gestion et par des compétences transverses, indispensables dans les cursus MIAGE.

L'originalité du MBDS est de développer le thème de la mobilité, source de nombreux travaux de recherche ou produit des entreprises en informatique.

Les objectifs scientifiques se situent à deux niveaux :

- Former des développeurs de Systèmes d'information du futur des bases de données (administration et tuning) au Big Data (gestion et architecture ; Hadoop)
- Intégrer les résultats les plus avancés en recherche sur les services web, les développements sur Smartphone (HTML5 comme code natif) et l'analyse de données (langage R)

La spécialité MBDS proposée est indifférenciée (Professionnelle et Recherche).

V.2 Présentation de la BRH (Banque de la République d'Haïti)

Nous présentons ici la BRH car c'est elle qui sera le gestionnaire de la gourde électronique. La Banque de la République d'Haïti ou BRH est une institution financière qui joue le rôle de banque centrale pour la République d'Haïti. À travers son Conseil d'Administration, elle a le pouvoir d'énoncer, de diriger et de superviser la politique monétaire. Elle autorise l'impression de billets et la frappe de monnaie et détermine les volumes des émissions en accord avec la loi.

La loi du 17 août 1979 portant création de la BRH dispose en son article 6 que celle-ci est dirigée par un Conseil d'Administration dont les membres sont nommés pour une période de trois ans renouvelables par arrêté du président de la République. Conformément aux dispositions de la Constitution de 1987, ils sont ratifiés par le Sénat de la République.

La législation en vigueur assigne quatre rôles fondamentaux à la BRH, lesquels peuvent être énoncés comme suit :

- Défendre la valeur interne et externe de la monnaie nationale
- Assurer l'efficacité, le développement et l'intégrité du système de paiements
- Assurer la stabilité du système financier
- Agir comme banquier, caissier et agent fiscal de l'État

VI. Etat de l'art

VI.1. La blockchain

VI.1.1. Définition

« La blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle.

Par extension, une blockchain constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne. » (Définition de Blockchain France)

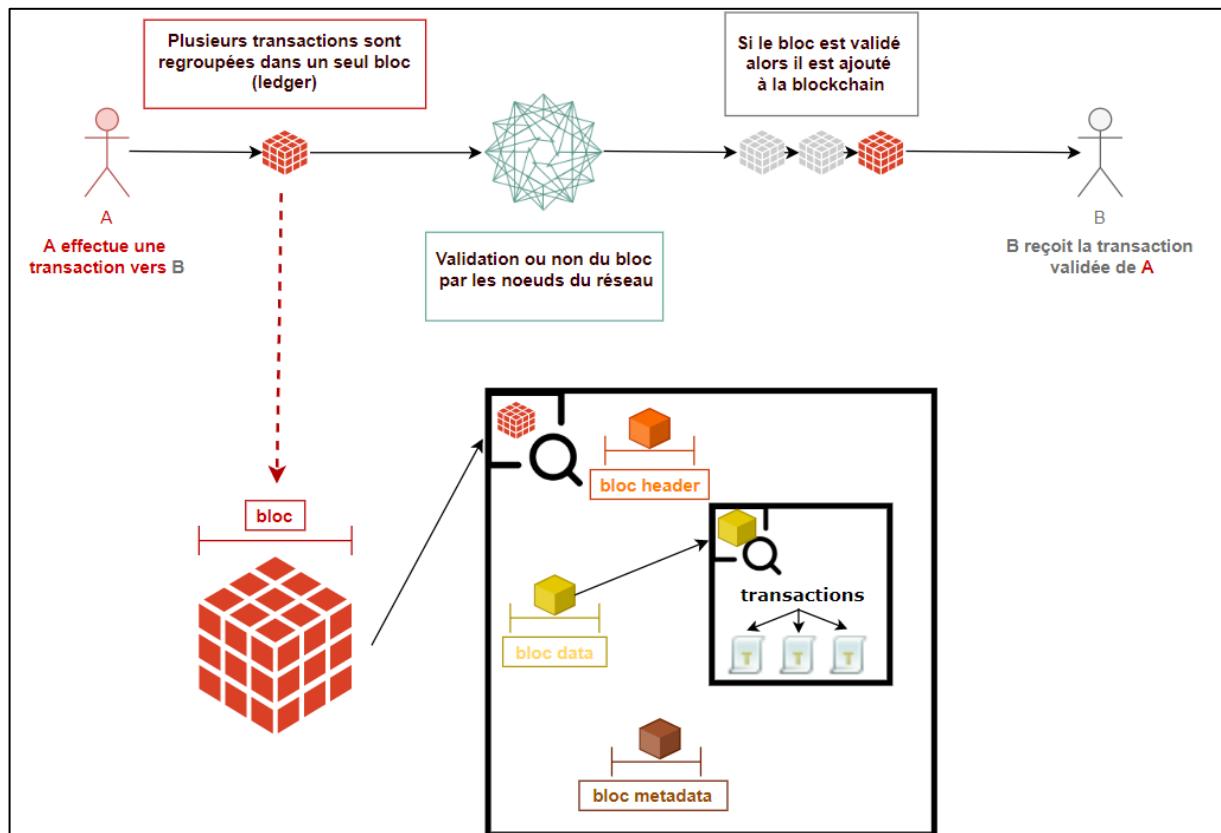


Figure 1 : Fonctionnement d'une blockchain

VI.1.2 Les règles de consensus

Les règles de consensus désignent le protocole selon lequel un individu sera choisi pour ajouter son bloc à la blockchain. Ce sont les règles de consensus qui assurent la sécurité du réseau et dissuadent la falsification des blocs.

	Description	Avantages	Inconvénients
PoW	Proof of Work : Preuve de travail. Dans une Blockchain publique, les ordinateurs des mineurs sont mis à disposition pour résoudre un problème mathématique compliqué. Le 1 ^{er} qui trouve une solution gagne la récompense du prochain bloc de la chaîne (12.5 bitcoin ou 5 ether).	<ul style="list-style-type: none"> Sécurisé, éprouvé et robuste. 	<ul style="list-style-type: none"> Très consommateur d'électricité et de matériel informatique.
PoS	Proof of Stake : Preuve d'enjeu. Les validateurs de transactions doivent mettre en gage la possession de crypto monnaie pour recevoir une récompense. Si un nœud est malveillant, il peut perdre sa mise en gage au profit des validateurs honnêtes.	<ul style="list-style-type: none"> Peu consommateur en ressources énergétiques. 	<ul style="list-style-type: none"> Peu testé à grande échelle.
PBFT	Practical Byzantine Fault Tolerant : Consensus dont la liste des validateurs est connue au départ et peut tolérer jusqu'à 1/3 de nœuds compromis (déconnectés ou malveillants).	<ul style="list-style-type: none"> Consensus de groupe rapide et performant. Pas de fork ou de réorganisation de chaîne. 	<ul style="list-style-type: none"> Chaine privée uniquement.
PoA	Proof of Authority : Preuve d'autorité. Consensus dont la liste des validateurs est connue au départ et qui valide à tour de rôle un bloc. Ce type de consensus peut tolérer jusqu'à 49% de nœuds malveillants ou déconnectés.	<ul style="list-style-type: none"> Consensus de groupe rapide. 	<ul style="list-style-type: none"> Chaine privée uniquement. Fork ou réorganisation de la chaîne possible.

Figure 2 : Les différentes règles de consensus (La Blockchain- Panorama des technologies existantes © 2017 Deloitte SAS)

VI.2 Les types de blockchains

VI.2.1 PUBLIQUE

La blockchain dites « publique » est la blockchain d'origine, elle est totalement décentralisée. C'est-à-dire que tout le monde peut lire, effectuer des transactions et participer au processus de validation de blocs, qui seront ou non ajoutés à la blockchain. Tous les acteurs sont égalitaires vis-à-vis de leur participation dans le réseau.

EXEMPLES : BITCOIN, ETHEREUM, LITECOIN, ETC.

VI.2.2 PRIVE ("DISTRIBUTED LEDGER TECHNOLOGY" (DLT))

Depuis 2015 les blockchains partiellement décentralisées ou centralisées se développent et offrent de nombreux avantages :

- Gouvernance simplifiée
- Acteurs connus
- Coûts réduits
- Rapidité
- Confidentialité

EXEMPLES : HYPERLEDGER, CORDA, MONEX, B3I, R3, LABCHAIN, ETC.

VI.2.2.1 BLOCKCHAIN DE CONSORTIUM (SEMI-PRIVE)

La blockchain dites « de consortium » limite et sélectionne le nombre de participants du processus d'approbation et la règle de la majorité ne s'impose pas. La lecture des blocs est publique, réservée

aux participants ou hybride. Ce type de blockchain est principalement utilisé dans le secteur bancaire.

EXEMPLES : R3 (BANQUES), EWF (ENERGIE), B3I (ASSURANCE), CORDA.

Il y a certains inconvénients, étant donné que la création de bloc est facilitée (une signature suffit), il est possible de créer autant de chaines que possible. De fait si l'on venait à ouvrir la blockchain en lecture à des tiers (clients, auditeurs), ceux-ci n'auraient aucun moyen de vérifier que les données qu'ils consultent soient en provenance de chaîne légitime. On pourrait donc se retrouver dans un système de Ponzi (montage financier frauduleux qui consiste à rémunérer les investissements des clients essentiellement par les fonds procurés par les nouveaux entrants).

VI.2.2.2 BLOCKCHAIN TOTALEMENT PRIVEE

La blockchain dites « privée » va autoriser un nombre limité et prédéfini d'acteurs. C'est une seule organisation qui va autoriser ou non la possibilité d'effectuer des transactions ou même de participer à la validation de blocs.

EXEMPLES : HYPERLEDGER FABRIC, CORDA, OPENCHAIN, ETC.

		Blockchain publique	Blockchain privée
 Usage		Nous préconisons l'usage d'une Blockchain publique pour gérer des traces simples (hash) pour une piste d'audit. Au-delà des traces simples, la Blockchain publique est moins pertinente compte tenu de son coût de manipulation des données et de ses limites dans la gestion de la confidentialité.	Nous préconisons l'usage d'une Blockchain privée pour gérer des échanges plus riches que de simples traces. L'absence de frais de transaction permet une taille des données stockées plus importante. En outre, la gestion des droits d'accès et de la confidentialité peut être davantage maîtrisée.
 Sécurité		Plus il y a d'utilisateurs, plus la sécurité de la Blockchain est garantie. Généralement, le consensus sur une Blockchain publique est garanti par la preuve de travail (PoW).	 Seuls les nœuds validateurs sont autorisés à valider une transaction. Un consensus de n% (par ex 2/3) des membres validateurs est requis.
 Confidentialité		Les données transitent de manière transparente. Sauf divulgation, les détenteurs des adresses sont anonymes (i.e. transactions semi-anonymes).	 Seuls les acteurs autorisés de la Blockchain privée ont accès aux transactions.
 Scalabilité		Entre 3 et 7 transactions financières par seconde mais une transaction peut contenir plusieurs milliers de hash grâce au processus de « Merkleisation ».	 1 000 transactions par seconde, voire plus.
 Accessibilité		« Permissionless » : comme internet, accessible à tous.	 Accès aux membres du consortium uniquement.
 Fort  Faible			

Figure 3 : Différences entre blockchain privée et publique (La Blockchain- Panorama des technologies existantes © 2017 Deloitte SAS)

VI.2.3 Critères relatifs à notre projet

Nous nous basons sur des blockchains existantes.

Les critères de comparaisons seront les suivants :

1. Type blockchain
2. Accès en lecture
3. Accès en écriture
4. Accès en modification

Type de blockchain	Lecture	Ecriture	Modification	Exemples d'utilisation
Publique	Tout public	Tout public	Tout public	Bitcoin
Consortium	Public restreint	Public restreint	Tout public ou Public restreint	Transactions entre plusieurs banques
Privé	Public restreint	Administrateur	Administrateur	Transaction au sein d'une seule banque

VI.3 La crypto-monnaie

VI.3.1 Définition

Une cryptomonnaie est une monnaie virtuelle, elle ne dispose donc pas de support physique. Elle permet de réaliser des transactions financières, des achats, des virements, ou du stockage de valeur, comme la monnaie traditionnelle.

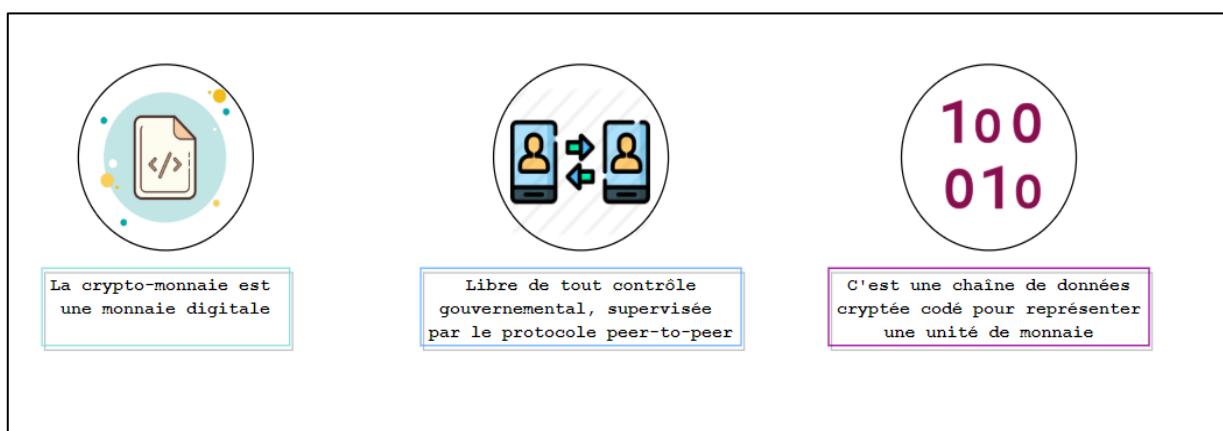
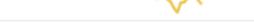


Figure 4 : Qu'est-ce que la crypto-monnaie ?

La cryptomonnaie est cryptée et peut être utilisée uniquement par les personnes détenant le code de décryptage. Il peut s'agir d'un mot de passe, d'une empreinte digitale ou de tout autre élément permettant de s'identifier. Contrairement à la monnaie classique, les transactions sont très rapides, très peu couteuses et se font dans l'anonymat total. Grâce au système de cryptographie, les transactions ne peuvent pas non plus être falsifiées.

VI.3.2 Les différentes crypto-monnaies

Ci-dessous un classement des crypto-monnaies en fonction de leur valorisation boursière.

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	\$146 332 622 941	\$8 103,55	\$22 244 596 010	18 057 850 BTC	-0,88%	
2	Ethereum	\$19 243 602 761	\$177,16	\$7 746 351 760	108 623 565 ETH	-0,20%	
3	XRP	\$10 924 871 813	\$0,252307	\$1 479 527 937	43 299 885 509 XRP *	1,14%	
4	Bitcoin Cash	\$4 395 876 126	\$242,56	\$2 084 961 161	18 123 038 BCH	-0,44%	
5	Tether	\$4 171 190 247	\$1,02	\$23 516 747 450	4 108 044 456 USDT *	1,06%	
6	Litecoin	\$3 560 330 253	\$55,88	\$3 101 880 016	63 719 521 LTC	-0,52%	
7	EOS	\$2 927 389 705	\$3,11	\$2 209 493 743	940 945 927 EOS *	-1,69%	
8	Binance Coin	\$2 881 527 481	\$18,53	\$213 120 186	155 536 713 BNB *	-1,68%	
9	Bitcoin SV	\$1 934 174 966	\$107,05	\$511 639 661	18 068 415 BSV	-3,81%	
10	Stellar	\$1 313 701 427	\$0,065506	\$275 619 086	20 054 779 554 XLM *	-0,60%	
11	TRON	\$1 129 948 618	\$0,016945	\$1 135 366 258	66 682 072 191 TRX	-0,56%	
12	Cardano	\$1 080 229 677	\$0,041664	\$82 983 672	25 927 070 538 ADA	-1,14%	
13	Monero	\$1 019 022 548	\$58,85	\$203 245 302	17 316 225 XMR	-0,40%	
14	Chainlink	\$973 405 086	\$2,78	\$182 492 677	350 000 000 LINK *	3,83%	

VI.3.3 Critères relatifs à notre projet

Nous nous basons sur des crypto-monnaies d'états en circulation.

Les critères de comparaisons seront les suivants :

- Plateforme : indique sur quelle blockchain la crypto-monnaie s'appuie
- Objectif : indique dans quel cadre la crypto-monnaie a été créée et quels sont les objectifs du projet

- Type blockchain : privée, publique ou de consortium
- Caractère social : indique si le projet pour lequel a été créé la crypto-monnaie est à but non lucratif

Crypto-monnaie	Plateforme	Objectif	Type	Caractère Social
Bitcoin	Bitcoin	Décentralisation du système bancaire	Public	Non
Ethereum	Ethereum		Public/Privé	Non
Petro	Nem	Se base sur le cours du pétrole et permet de payer son dû à l'état (impôts,etc.)	Privé	Oui
Paypite	Ethereum	Rendre les transactions plus rapides, moins chers et transparents	Privé	Oui
Digital Gourde	OpenChain	Permettra à tous les citoyens d'être bancarisés	Privé	Oui

VII. Etude de l'existant

VII.1 L'environnement

VII.1.1 Openchain

En se basant sur les versions précédentes du projet, la blockchain choisie est Openchain.

VII.1.1.1 Fonctionnement

Openchain est une technologie de blockchain open source, ou plutôt chaîne de transaction. En effet, Openchain n'utilise pas le concept de bloc vu plus haut, les transactions sont directement groupées entre elles et non via des blocs. Cela permet de gagner en temps et les transactions sont validées en (quasi) temps réel.

Caractéristiques propres à Openchain :

- Validation instantanée des transactions
- Pas de frais de minage
- Scalabilité extrêmement élevée
- Sécurisé via signatures numériques
- Attribution d'alias aux utilisateurs au lieu d'utiliser des adresses en base 58
- Plusieurs niveaux de contrôle :
 - Un registre entièrement ouvert pouvant être rejoint anonymement
 - Les participants doivent être approuvés par l'administrateur
 - Certains utilisateurs jouissent de plus de droits que les utilisateurs anonymes
- Système de hiérarchie
- Transparence des transactions
- Gestion de la perte ou du vol de clés privées pour les utilisateurs finaux
- Possibilité d'avoir plusieurs instances d'Openchain

VII.1.2 API

Le serveur Openchain expose une API HTTP pouvant être utilisée pour interagir avec les données. L'URL d'une opération est construite à partir de l'URL de base du nœud final et du chemin d'accès relatif de l'opération.

Par exemple, si l'URL de base est <https://www.openchain.org/endpoint/>, pour appeler l'opération/record (interroger un enregistrement), l'URL complète sera <https://www.openchain.org/endpoint/record>.

Quelques opérations utiles :

- Soumettre une transaction ([/submit](#))
- Interroger un enregistrement ([/record](#))
- Flux de transactions ([/stream](#))
- Récupérer les informations sur la chaîne ([/info](#))
- Interroger un compte ([/query/account](#))
- Interroger une transaction ([/query/transaction](#))
- Interroger une version spécifique d'un enregistrement ([/query/recordversion](#))
- Interroger toutes les mutations ayant affecté un enregistrement ([/query/recordmutations](#))
- Interroger les enregistrements dans un compte et ses sous-comptes ([/query/subaccounts](#))
- Interroger tous les enregistrements avec un type et un nom donné ([/query/recordsbyname](#))

Dans ce projet, le traitement des requêtes HTTP venant du client Angular passe par une API Restful constituée de :

1. Un serveur avec Node.js et le Framework Express.js
2. Une base de données MySQL

VII.1.2 Hyperledger Fabric, une alternative à Openchain

VII.1.2.1 Concepts

Hyperledger Fabric est une blockchain Open Source, extrêmement modulaire, proposée par la Linux Foundation et spécialement conçue pour un usage privé et professionnel. Elle s'organise autour de plusieurs concepts :

- Organisation : acteur de la chaîne
- Nœud : un nœud du réseau, appartient à une organisation qui est chargée de maintenir son fonctionnement
- Brick : chargée d'organiser la vie du réseau
- Channel : « sous blockchain » dans laquelle sont inscrits les blocs en fonction du sujet
- CA : brick chargée de vérifier les certificats
 - o Ajouter des identités
 - o Générer des certificats
 - o Renouveler ou révoquer des certificats
- Blocs cachés (private data) : permet de créer des données privées dans un channel au lieu de créer un nouveau channel, on peut donc partager un même channel entre plusieurs organisations
- Cycle de vie du Chaincode

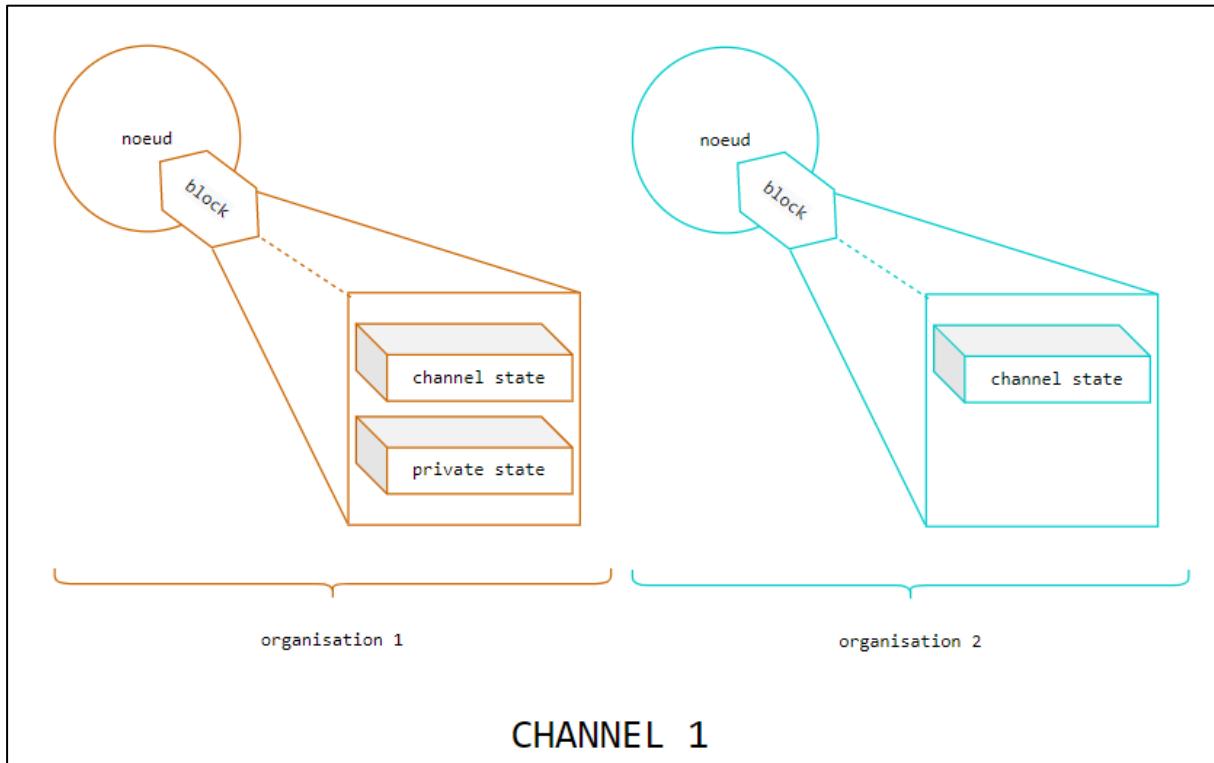


Figure 6 : Schématisation d'un bloc caché

VII.1.2.2 Architecture

A la différence de OpenChain, Hyperledger Fabric contient un « bloc » contenant les états finaux de chaque objet afin d'alléger la charge d'un bloc (contient tous les fichiers, transactions, etc.)

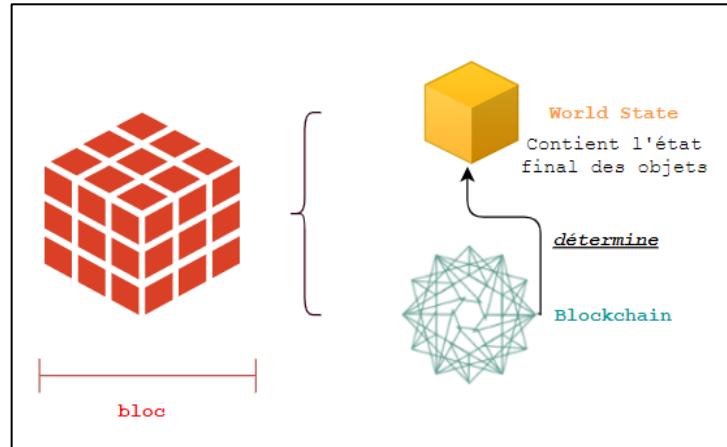


Figure 7 : Architecture Hyperledger Fabric

VII.1.2.3 Architecture du PoC (proof of concept)

Le PoC est composé de différents éléments :

- Une instance Hyperledger vierge
- Un server Node.js
- Un système de Push Notifications Web
- Une PWA

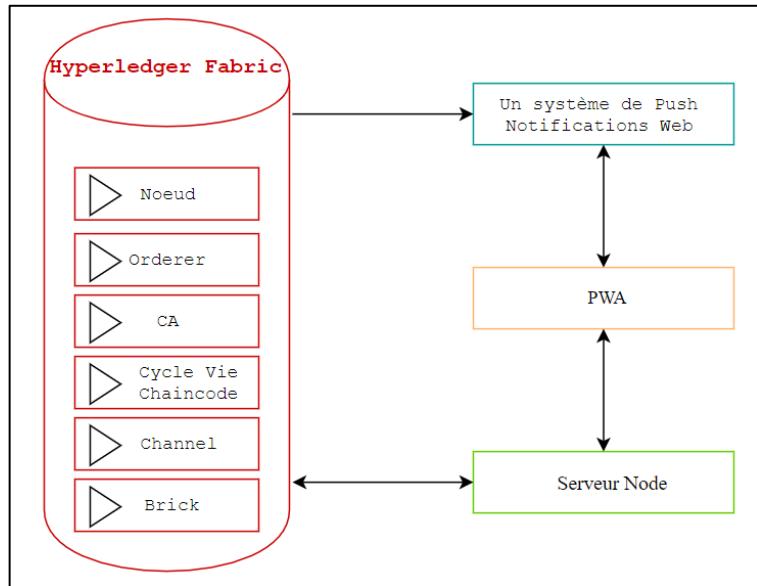


Figure 8 : Fonctionnement PoC

VII.1.2.4 Conclusion

Hyperledger Fabric semble convenir parfaitement à ce que nous voulons dans notre projet.

Dans notre cas, la blockchain est déjà implémentée et le temps imparti ne nous permet pas de changer de technologie. Or, elle serait intéressante à mettre en place dans une future version de l'application.

VII.1.3 MySQL – API REST NodeJs – Angular 7

Les détails des environnements utilisés sont disponibles en [Annexe : Documentation Technique de l'environnement existant](#)

VIII. Démarche projet

VIII.1 Gestion de projet

Dans le cadre de ce projet nous n'avons pas suivi de méthode précise de gestion de projet. Mais afin de s'assurer de l'avancement du projet de manière évolutive et très organisée il a été divisé en sprint.

La gestion du projet s'effectue directement sur GitHub avec les outils intégrés.

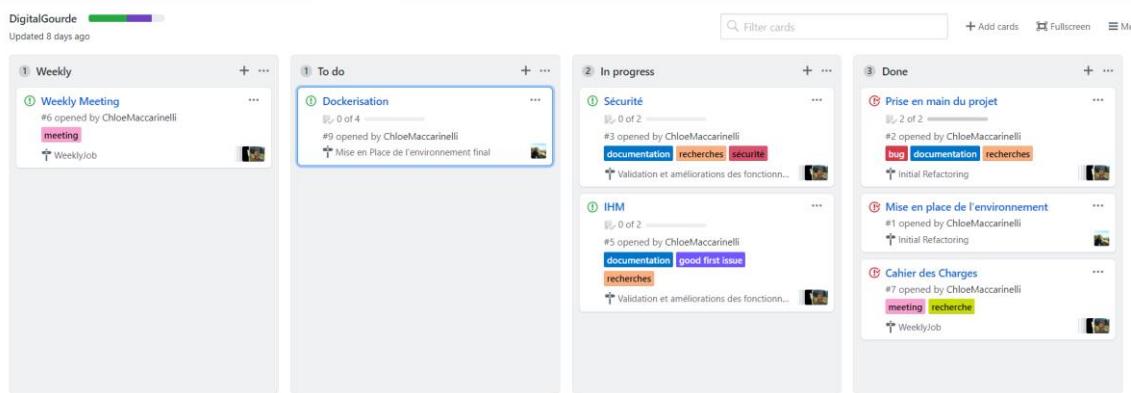


Figure 9 : Kanban DigitalGourde

VIII.2 Contraintes, outils et risques

VIII.2.1 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 REGLES SUIVANTES DOIVENT ETRE RESPECTEES

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 :

- La banque centrale ne peut distribuer aux institutions financières plus que le montant restant émis en gourde électronique disponible dans son portefeuille
- Une institution financière ne peut distribuer à ses clients plus que ce qu'elle possède dans son portefeuille
- 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

Quelle que soit l'opération, on débite toujours un portefeuille pour créditer un autre portefeuille

Un portefeuille est toujours rattaché à une banque

VIII.2.2 Outils

Pour la réalisation de ce projet nous avons utilisé les outils suivants :

- IntelliJ
- Github
- Android Studio
- GanttProject
- Docker

VIII.2.3 Risques

Par définition, un risque est un danger éventuel, plus ou moins prévisible, inhérent à une situation ou à une activité. L'idée du plan de risque est d'anticiper et de limiter au maximum les risques qui pourraient survenir pour tenter de réduire leurs impacts sur le bon déroulement du projet, vu qu'il est fort probable que le projet ne se réalise pas selon les prévisions et que le risque zéro n'existe pas.

Libellés	Pri ori té	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 mobile complet	5	-Cahier des charges non définies -Le temps imparti pour la réalisation du projet	- Implémenter les cas d'utilisation les plus importants - Délai supplémentaire - Simplification des fonctionnalités	En cours / 20/02/2020	20JH

** Pour une blockchain privée ou semi-privée déjà existante type Hyperledger, Quorum ou **Corda**, les coûts seront liés aux développements nécessaires pour implémenter les modules et les fonctionnalités voulues ainsi que des **coûts de licence** et de maintenance. Pour l'implémentation d'une blockchain sur mesure “from scratch”, les coûts sont liés à du développement et au **maintien des serveurs** principalement. (entre 200 et 600 euros par mois)

VIII.3 Planning

Vous trouverez ci-dessous la planification sous forme de diagramme de Gantt, et le planning prévisionnel.

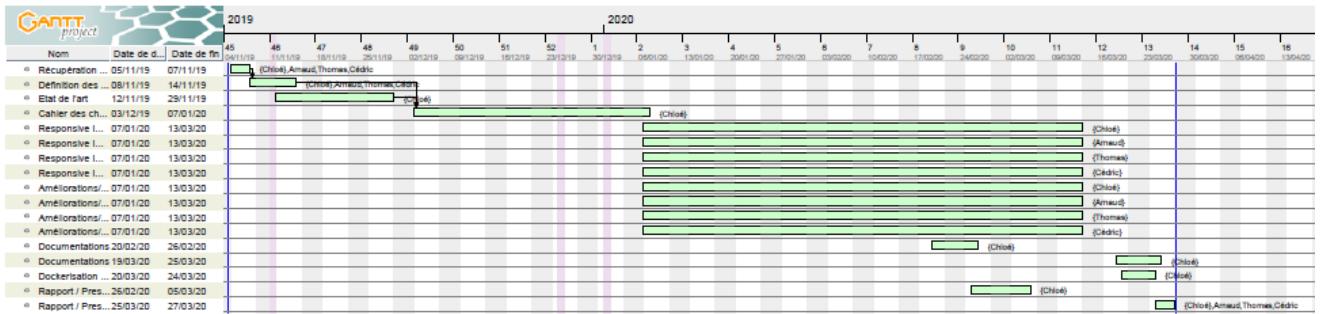


Figure 10 : Diagramme de Gantt

Élaboration du cahier des charges	15/11/2019
Etat de l'art	au
Prise en main du projet	01/02/2020
Mise en place de l'environnement et nouvelle technologie (Flutter)	
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 d'environ 18 Jours Homme par mois sur 5 mois, on estime le coût du projet à environ $18\text{JH} * 5 \text{ mois} = 90\text{JH}$.

	Nom ou Rôle	Jours Dispos	nov 2019	déc 2019	janv 2020	févr 2020	mars 2020
R1	Chef de projet	64	14	11	11	14	14
R2	Développeur 1	9	2	2	1	2	2
R3	Développeur 2	9	2	2	1	2	2
R4	Développeur 3	9	2	2	1	2	2
Total Jours		91	20	17	14	20	20
	Jours Ouvres	64	14	11	11	14	14
	Jours Féries						
	Jours travaillés	64	14	11	11	14	14

Figure 11 : Estimation du nombre de jours de travail

VIII.4 Budget

coût du Projet DIGITAL GOURDE			
Équipe:	R1	Chef de projet	
	R2	Développeur 1	
	R3	Développeur 2	
	R4	Développeur 3	
Date Début:	1-Nov-19		
Date Fin Prévue:	30-Mar-20		
coût Journalier du Travail:	150 €		
Consultant/Formations:	300 €	coût Travail + Formation(intervention tuteurs)	
Machines:	10 €		
Estimation			
Elément du coût	Unité/Jour	Coût(K€)	Notes
Travail	91	13,7K€	
Machines	91	0,9K€	
Formation	5	1,5K€	
Autres coûts	5	5,0K€	éclairages, locaux, etc
Total	192	21,1K€	

Figure 12 : Estimation du coût du projet

IX. Exigences fonctionnelles

Les exigences fonctionnelles définissent les caractéristiques fonctionnelles que l'application fournit aux entités extérieures interagissant avec elle, appelées "acteurs".

Une exigence fonctionnelle définit :

- Une information gérée par l'application
- Un comportement ou une fonction réalisée par l'application, appelé "cas d'utilisation".

Les cas d'utilisation décrivent les interactions de l'application avec ses acteurs.

IX.1 Les acteurs de niveau fonctionnel

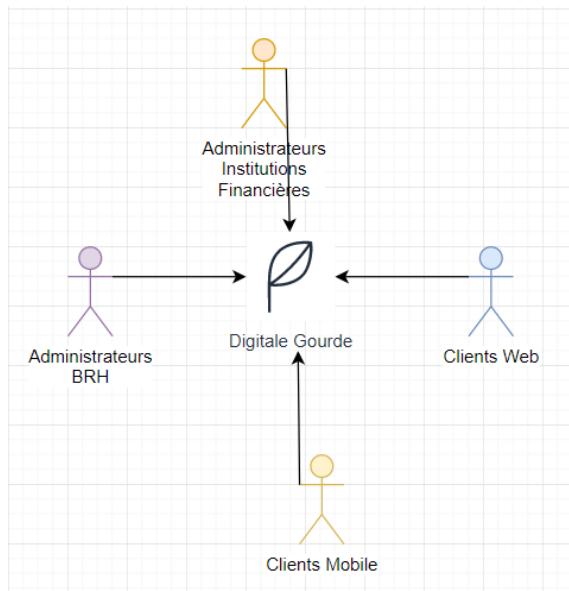


Figure 13 : Les acteurs

Client Web et mobile : personne qui utilise le système pour effectuer des transactions

Administrateur BRH : Ce sont les plus grands administrateurs, ce sont eux qui font les premières transactions et déterminent le nombre de cryptomonnaie en circulation avec l'accord de la BRH.

Administrateur Institutions Financières : personne responsable de la paramétrisation du système et de la distribution des droits d'accès de l'instance validateur dont il contrôle.

IX.2 Les cas d'utilisation

IX.2.1 Cas d'utilisation particuliers et commerçants (Partie Web)

Un commerçant doit être en mesure d'effectuer toutes les opérations qu'un particulier peut effectuer. A contrario un particulier ne peut pas effectuer toutes les opérations que peut effectuer un commerçant (réception de paiement, réception de dépôt en DHTG physique).

IX.2.1.1 Cas numéro 1

Un commerçant/particulier doit pouvoir se connecter à son espace personnel depuis l'application web et/ou mobile.

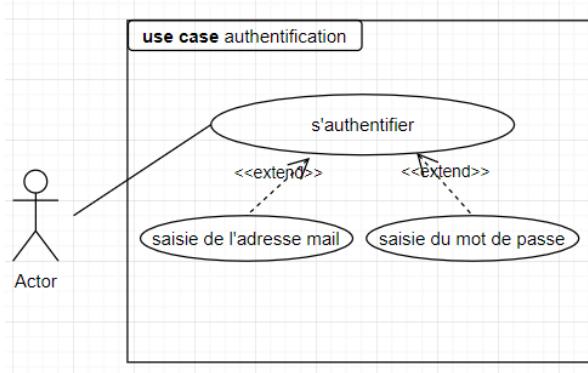


Figure 14 : Use Case authentification

Description détaillée

Résumé : Ce CU décrit l'authentification d'une personne au système.

Acteurs : Client web ou administrateur

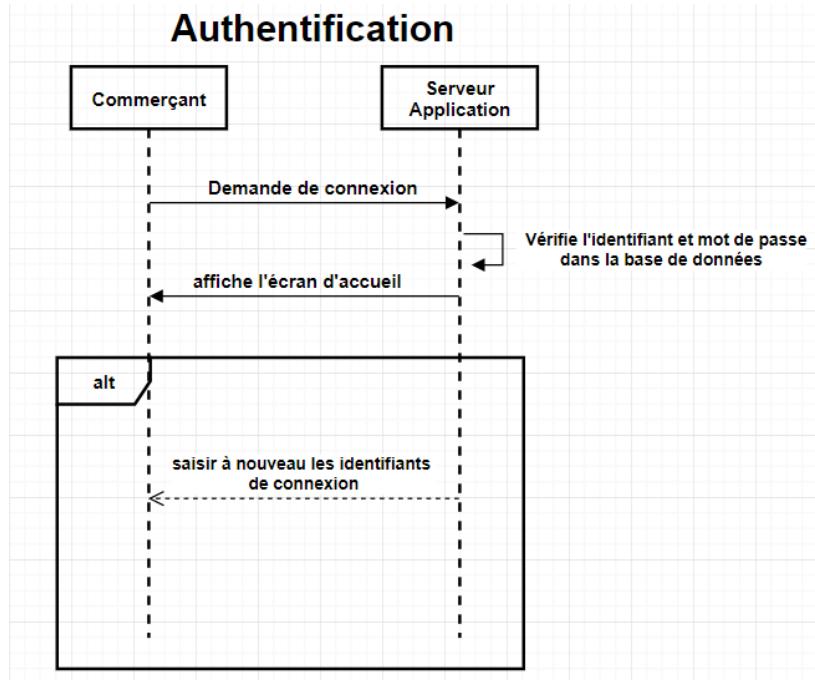
Précondition : Le client possède un portefeuille

Post condition : Le client est connecté à son portefeuille

Déroulement normal

Le CU commence quand le client veut s'authentifier. Il entre son adresse mail et mot de passe. L'application affiche l'écran accueil.

Le cas d'utilisation est terminé

*Figure 15: Diagramme de séquence authentification*

PAGE DE CONNEXION PARTICULIER/COMMERÇANT

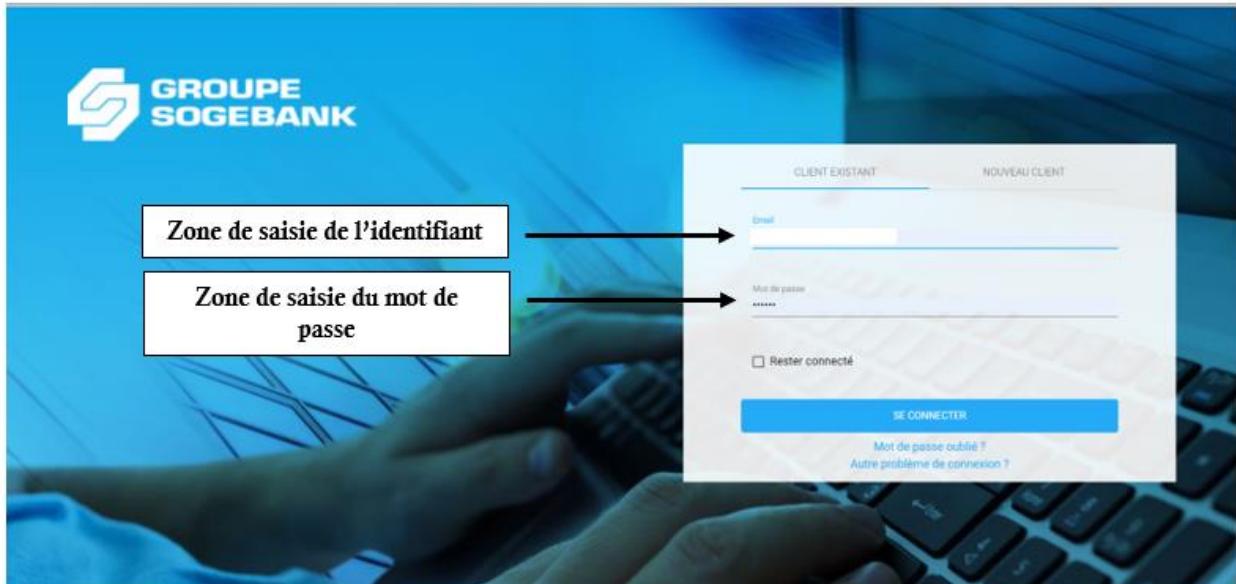
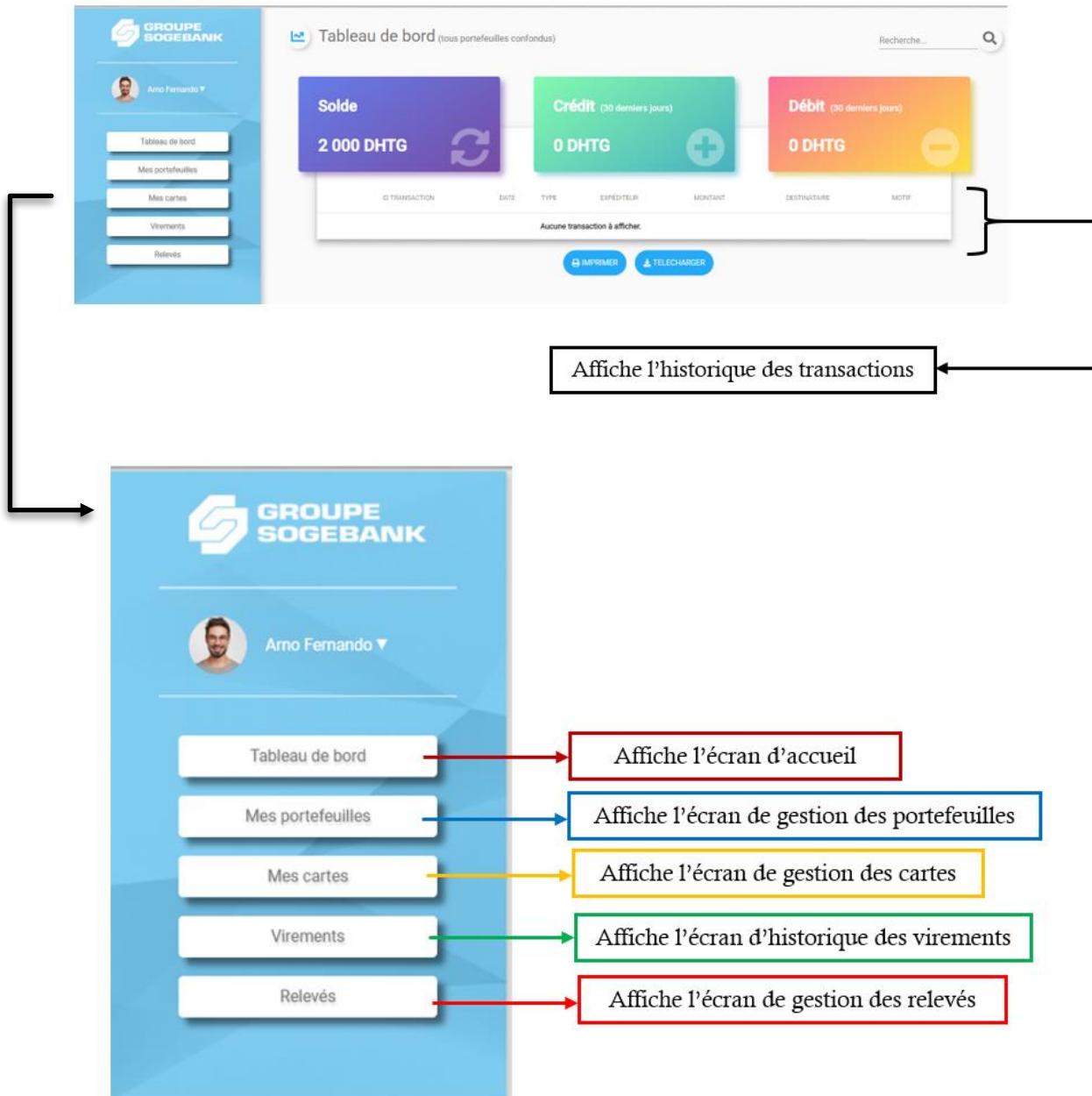


TABLEAU DE BORD D'ACCUEIL PARTICULIER/COMMERÇANT



VII.2.1.2 Cas numéro 2

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.

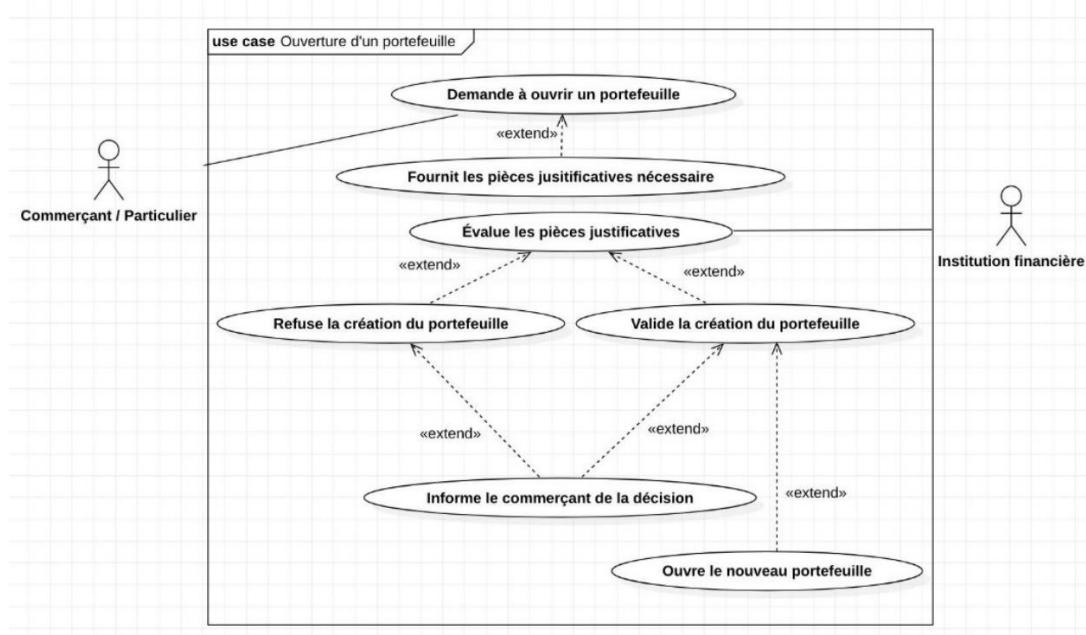


Figure 16 : Use Case ouverture de portefeuille

Description détaillée

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

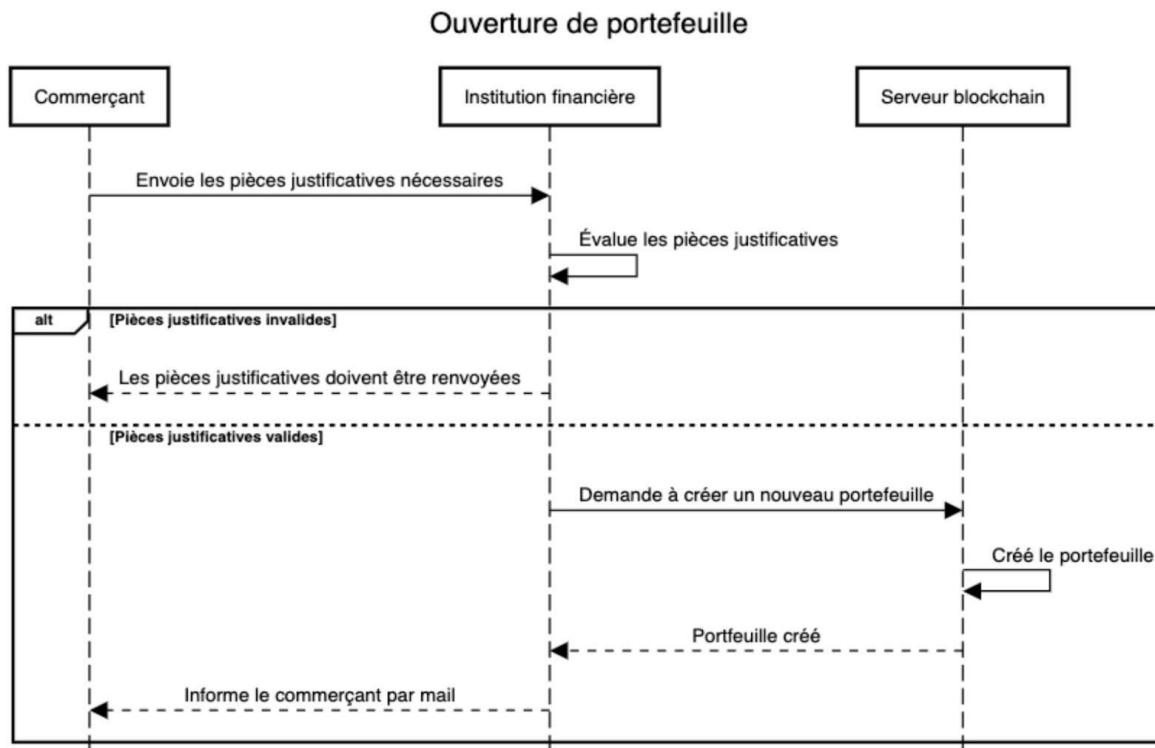
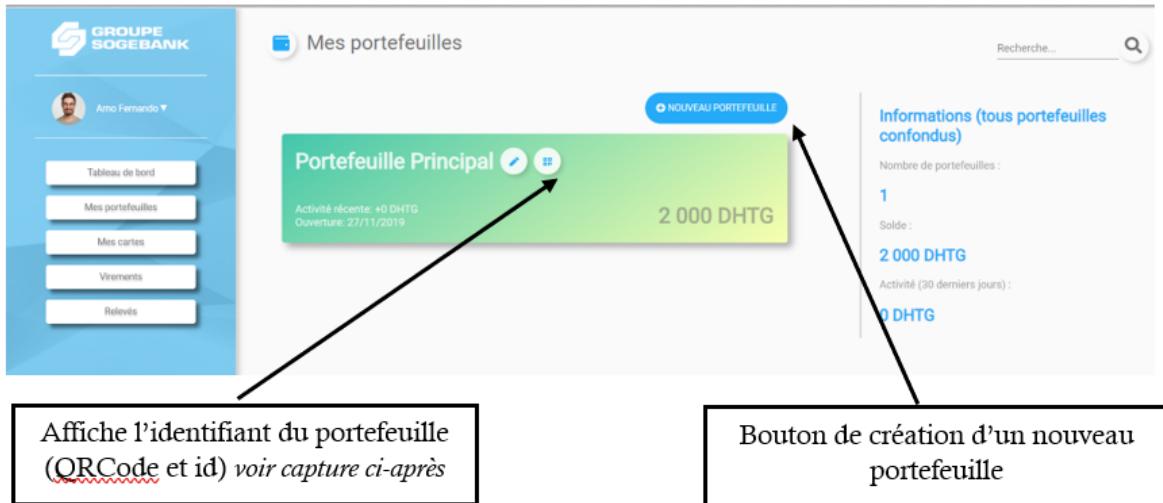


Figure 17 : Diagramme de séquence Ouverture de portefeuille

PAGE DE GESTION DES PORTEFEUILLES



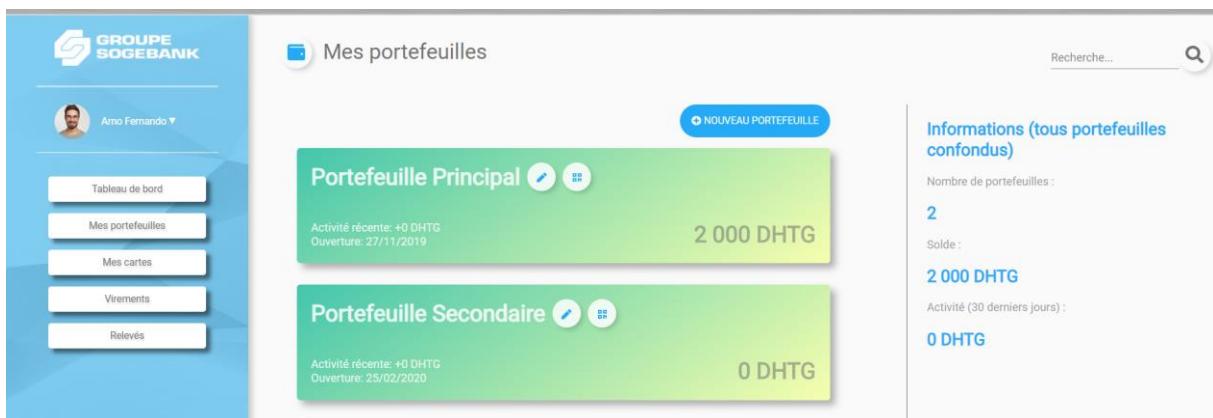
IDENTIFIANT D'UN PORTEFEUILLE NECESSAIRE POUR LES TRANSACTIONS



MODALE DE CREATION D'UN PORTEFEUILLE



LE PORTEFEUILLE EST CREE



VII.2.1.3 Cas numéro 3

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.

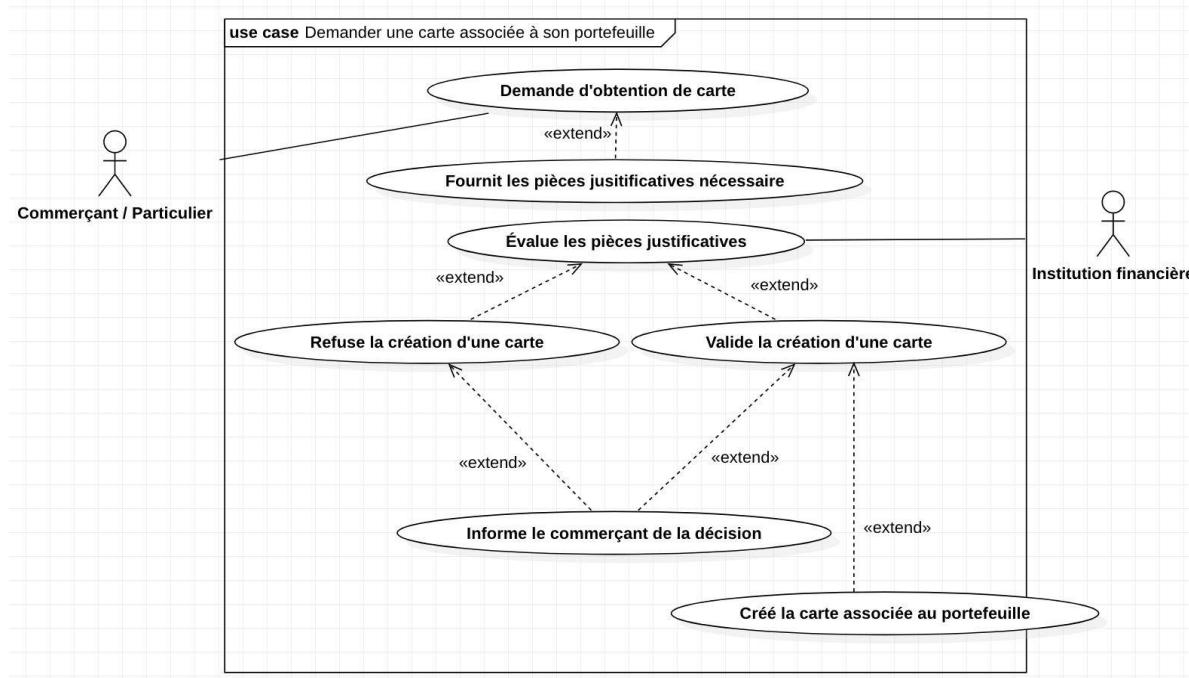


Figure 18 : Use case demande de carte

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

Demande de carte

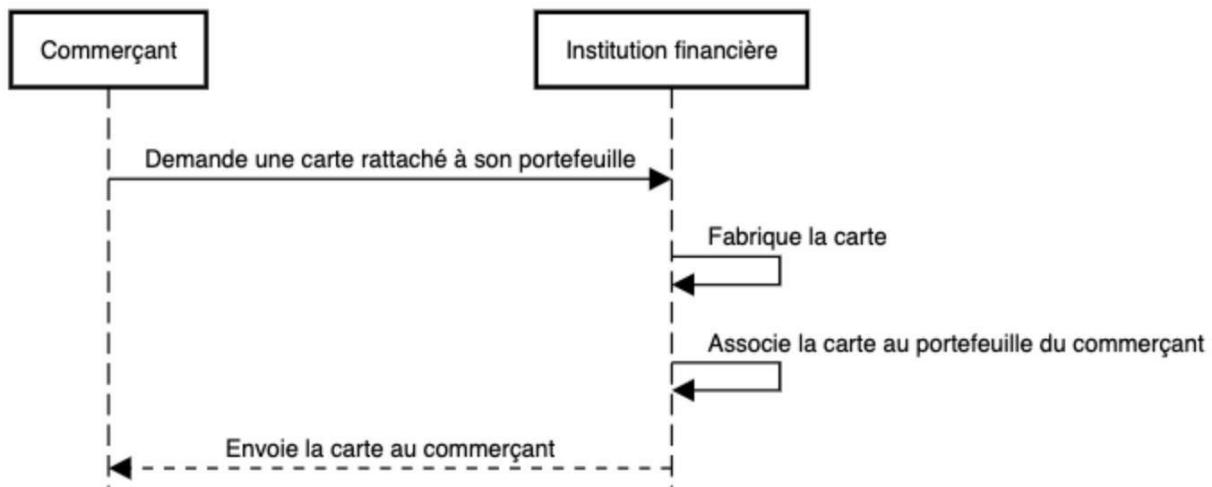
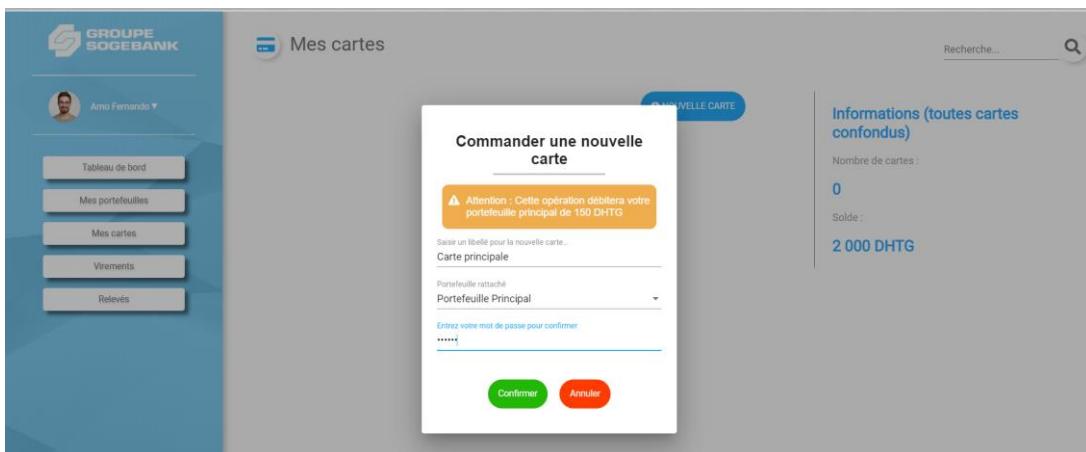
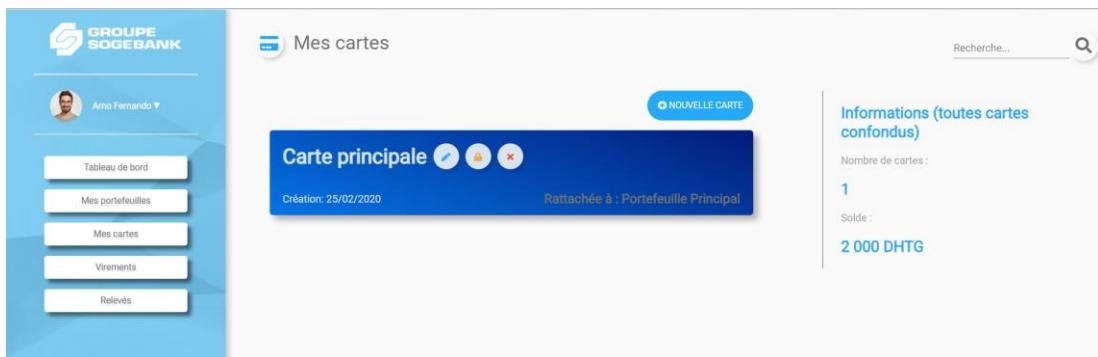


Figure 19 : Diagramme de séquence demande de carte

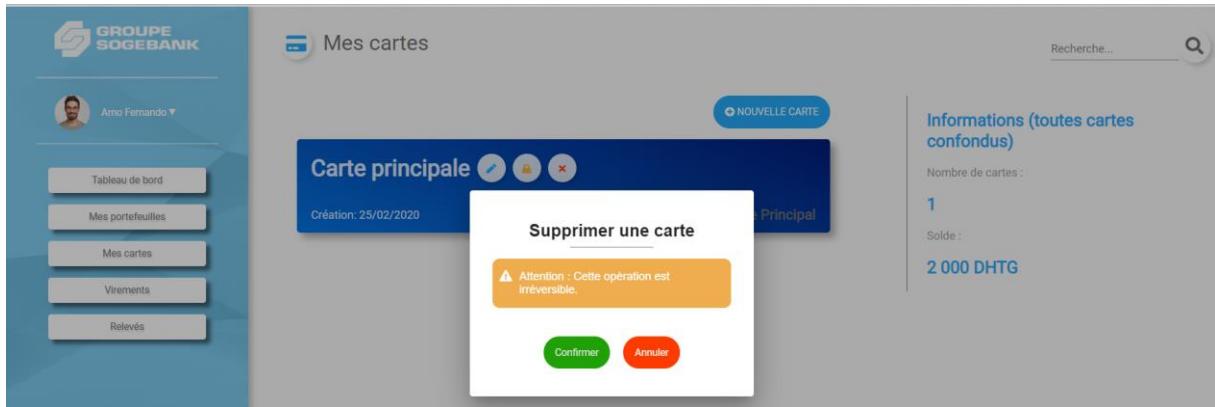
PAGE DE GESTION DES CARTES



LA CARTE EST CREEE



LA CARTE PEUT ETRE SUPPRIMEE



VII.2.1.4 Cas numéro 4

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.

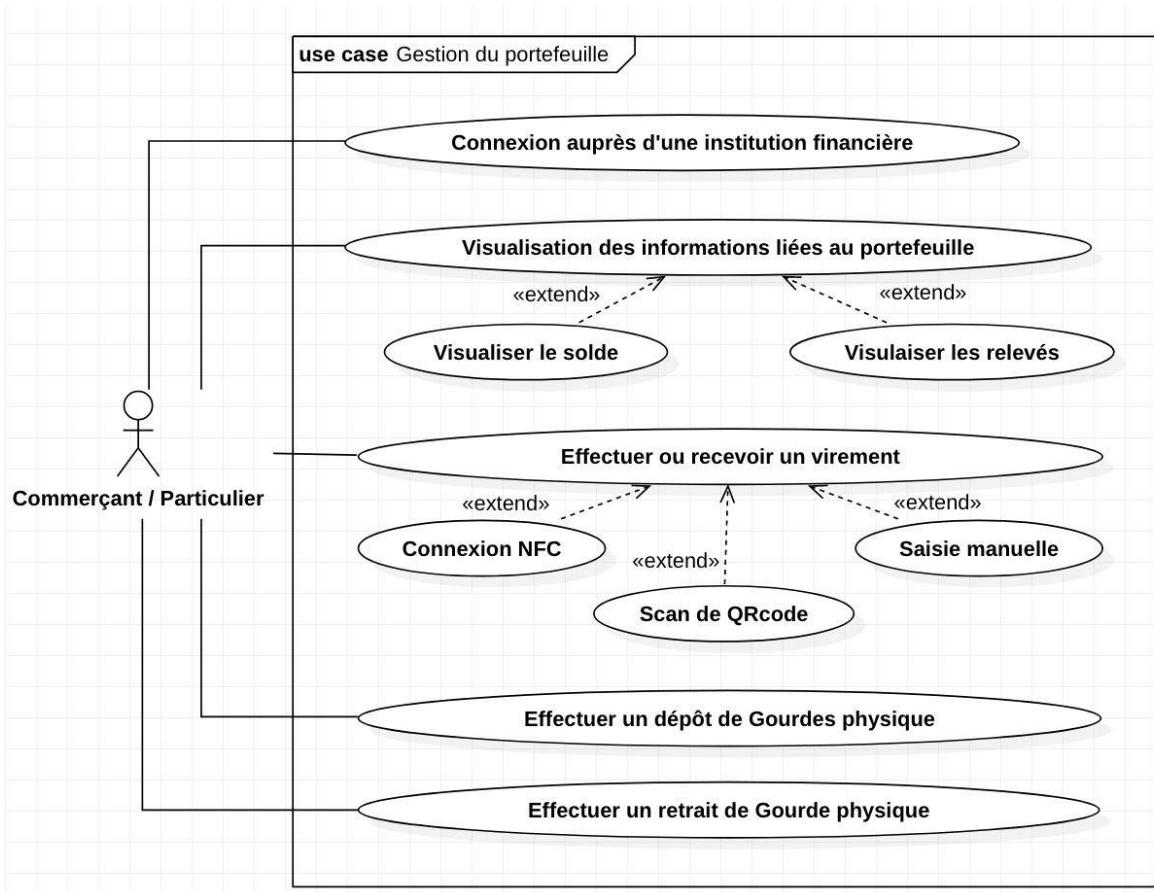


Figure 20 : Use case gestion du portefeuille

VII.2.1.4.1 Cas numéro 4.1

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

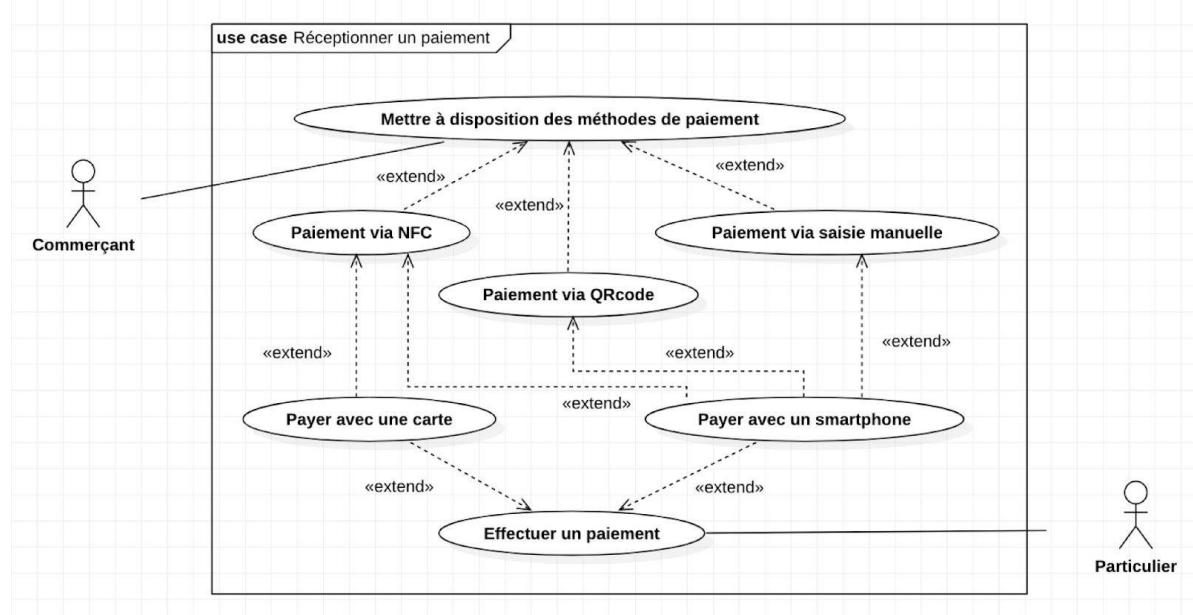


Figure 21 : Use case réception de paiement

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

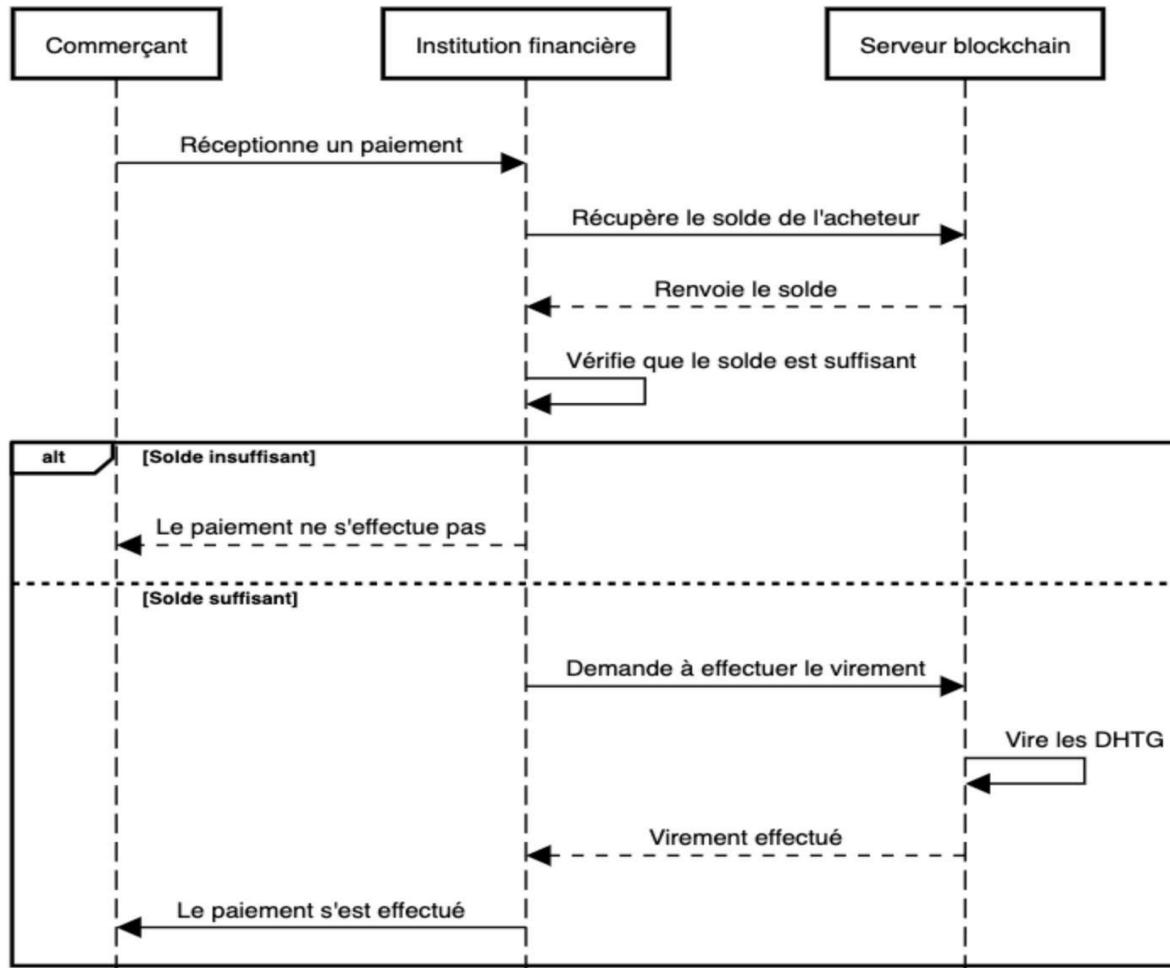
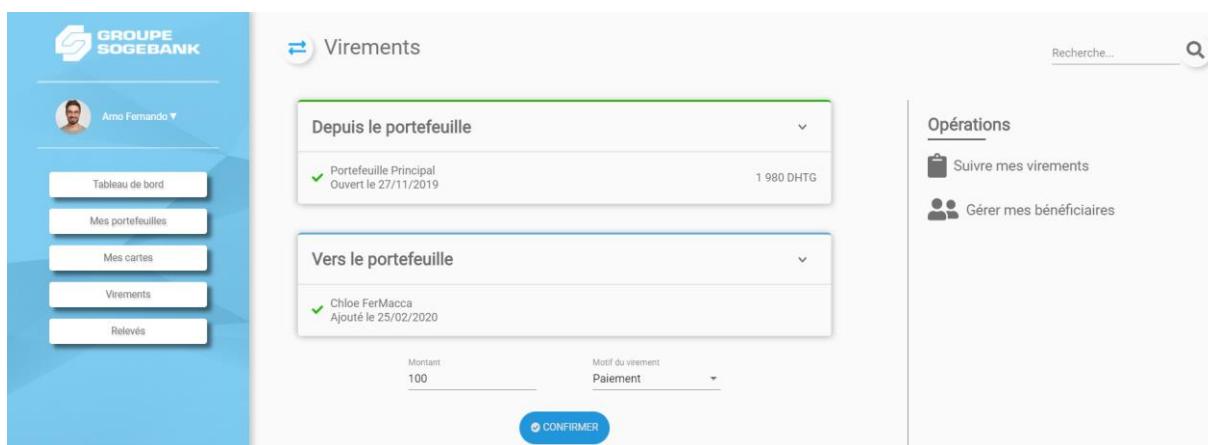


Figure 22 : Diagramme de séquence réception de paiement

VIREMENT EFFECTUE VERS UN TIERS (BENEFICIAIRE) ICI LE VIREMENT EST DEFINI COMME UN PAIEMENT



DEBIT DE 100 DHTG VERS UN TIERS (PARTICULIER)

The screenshot shows the Sogebank digital wallet interface. On the left, there's a sidebar with the Groupe Sogebank logo and a profile picture of Amélie Fernando. The main area is titled "Tableau de bord (tous portefeuilles confondus)". It displays three summary boxes: "Solde" (1 900 DHTG), "Crédit (30 derniers jours)" (20 DHTG), and "Débit (30 derniers jours)" (-120 DHTG). Below these are transaction details:

ID TRANSACTION	DATE	TYPE	EXPÉDITEUR	MONTANT	DESTINATAIRE	MOTIF
c79ffccc2d60f1f...	25/02/2020	Virement	Portefeuille Principal	-100 DHTG	Chloé FerMacca	Paiement
d7a699e619fc7b...	25/02/2020	Virement	Portefeuille Principal	-20 DHTG	Portefeuille Secondaire	Dépôt HTG
d7a699e619fc7b...	25/02/2020	Virement	Portefeuille Principal	+20 DHTG	Portefeuille Secondaire	Dépôt HTG

At the bottom are "IMPRIMER" and "TELECHARGER" buttons.

CREDIT DE 100 DHTG VENANT D'UN TIERS (COMMERÇANT)

The screenshot shows the Sogebank digital wallet interface. On the left, there's a sidebar with the Groupe Sogebank logo and a profile picture of Chloé FerMacca. The main area is titled "Tableau de bord (tous portefeuilles confondus)". It displays three summary boxes: "Solde" (2 100 DHTG), "Crédit (30 derniers jours)" (100 DHTG), and "Débit (30 derniers jours)" (0 DHTG). Below these are transaction details:

ID TRANSACTION	DATE	TYPE	EXPÉDITEUR	MONTANT	DESTINATAIRE	MOTIF	REQU
c79ffccc2d60f1f...	25/02/2020	Virement	Inconnu	+100 DHTG	Portefeuille Principal	Paiement	

At the bottom are "IMPRIMER" and "TELECHARGER" buttons.

VII.2.1.4.2 Cas numéro 4.2

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 QR code), un particulier doit pouvoir les déposer.

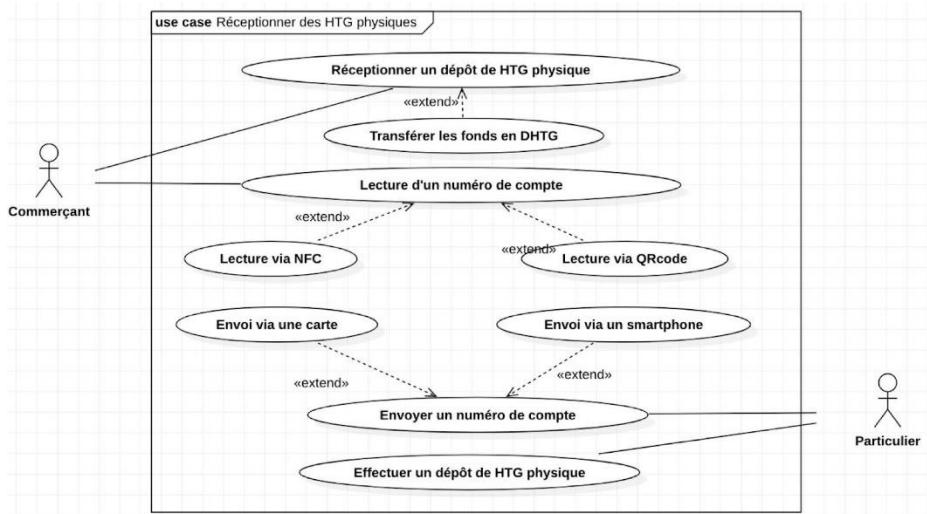


Figure 23 : Use case réception DHTG

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 versement 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

Réception de gourdes physiques

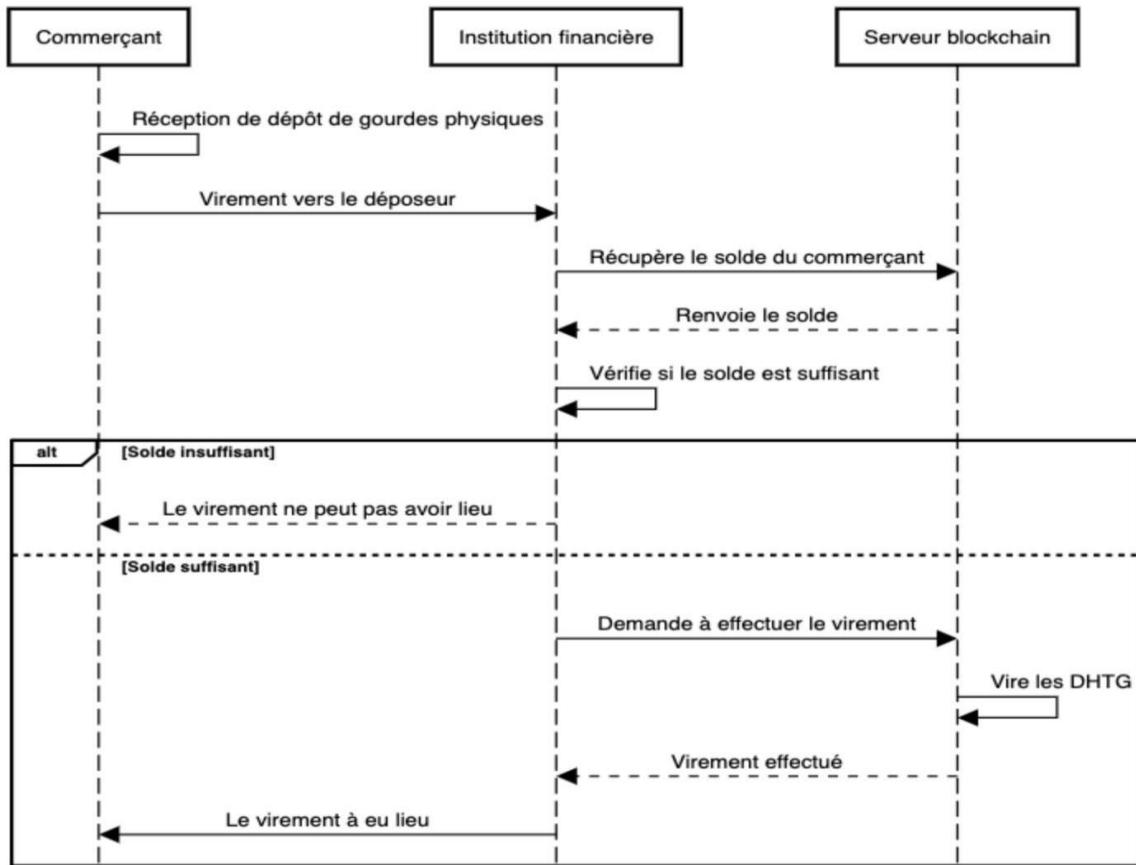


Figure 24 : Diagramme de séquence réception DHTG

VII.2.1.4.3 Cas numéro 4.3

Un commerçant, un particulier doit être en mesure d'effectuer un virement vers un autre compte du système.

Description détaillée

Résumé : Ce CU décrit le transfert de fonds vers un autre compte.

Acteurs : Client Web(particuliers/commerçants) ou Administrateurs

Précondition : Avoir un portefeuille actif

Post condition : Un crédit en DHTG sur le compte de réception et inversement pour le compte d'émission.

Déroulement normal :

Le commerçant/particulier saisie le montant à virer, la banque vérifie le solde du portefeuille à débiter, ainsi que l'existence du portefeuille à créditer. Si le solde est suffisant le virement est effectué sinon refusé.

Le cas d'utilisation est terminé

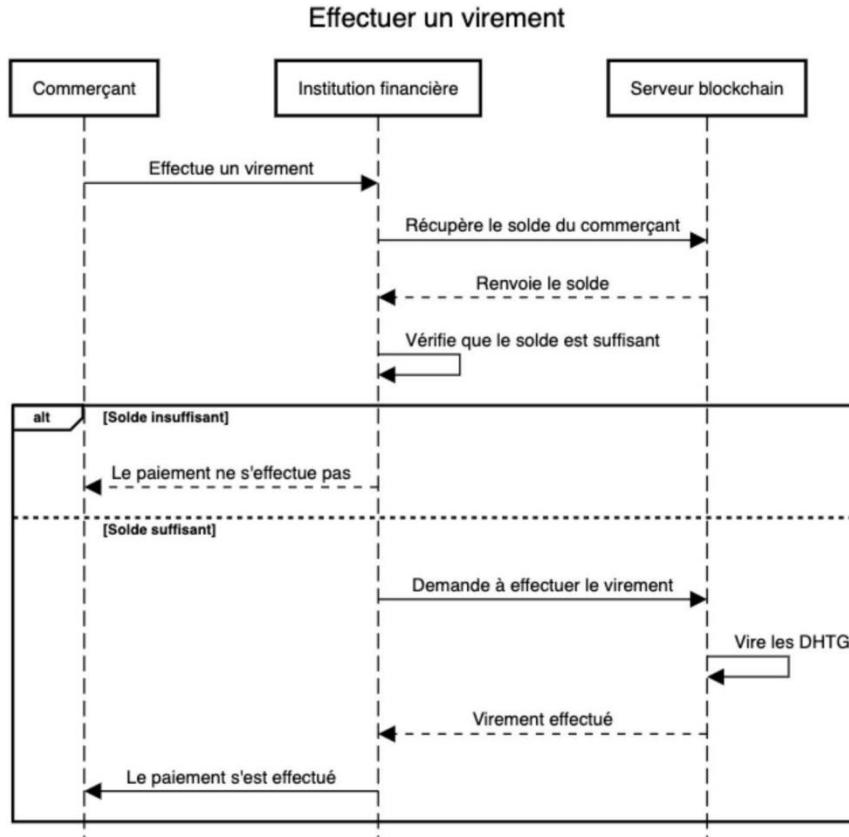


Figure 25: Diagramme de séquence effectuer un virement

[Voir IHM du Cas numéro 4.1.](#)

VII.2.1.4.4 Cas numéro 4.4

Un commerçant, un particulier doit être en mesure de visualiser son relevé bancaire pour un période donnée.

Description détaillée

Résumé : Ce CU décrit la visualisation du relevé

Acteurs : Client Web(particuliers/commerçants) ou Administrateurs

Précondition : Avoir un portefeuille actif

Post condition : Un relevé au format pdf ou imprimé

Déroulement normal :

Le commerçant/particulier saisi la date concernnée et choisi d'imprimer ou enregistrer son relevé bancaire.

Le cas d'utilisation est terminé

Visualiser son relevé

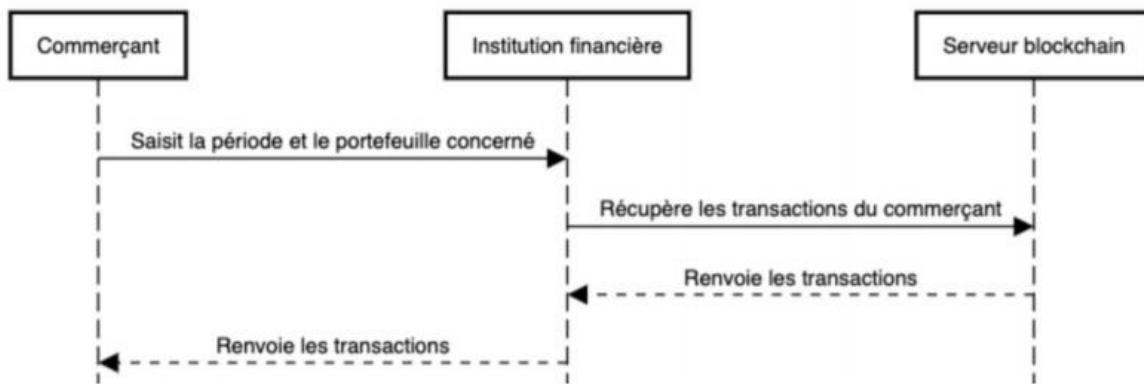


Figure 26 : Diagramme de séquence visualiser son relevé

PAGE DE GESTION DES RELEVES



IX.2.2 Cas d'utilisation particuliers et commerçants (Partie Mobile)

Un commerçant doit être en mesure d'effectuer toutes les opérations qu'un particulier peut effectuer. A contrario un particulier ne peut pas effectuer toutes les opérations que peut effectuer un commerçant (réception de paiement, réception de dépôt en DHTG physique).

Les cas d'utilisations de l'application mobile sont identiques aux cas de l'application web à l'exception du cas suivant (spécifique au mobile) :

IX.2.2.1 Cas numéro 1

Un particulier doit pouvoir payer un commerçant via l'application mobile (QR code)

Description détaillée

Résumé : Ce CU décrit le paiement via QR code

Acteurs : Client Mobile(particuliers/commerçants)

Précondition : Avoir un portefeuille actif

Post condition : Paiement effectué

Déroulement normal :

Le client clique sur le bouton Payer une commande. Le système affiche la liste des portefeuilles. Le client choisit un portefeuille. Le système génère un QR CODE associé au portefeuille choisi. Le commerçant saisit sur son lecteur de QR CODE le montant à payer. Le commerçant lit le QR CODE avec son appareil. Le système vérifie la validité de la transaction. Le système affiche un message de confirmation.

Le cas d'utilisation est terminé

IX.2.3 Cas d'utilisation institutions financières

1. CAS D'UTILISATION SIMILAIRES A CEUX DES PARTICULIERS

- 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)

2. CAS D'UTILISATION SPECIFIQUES AUX INSTITUTIONS FINANCIERES

- 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, ...)
- Demander une habilitation à la banque centrale (attention justificatifs) depuis le site web de la banque centrale

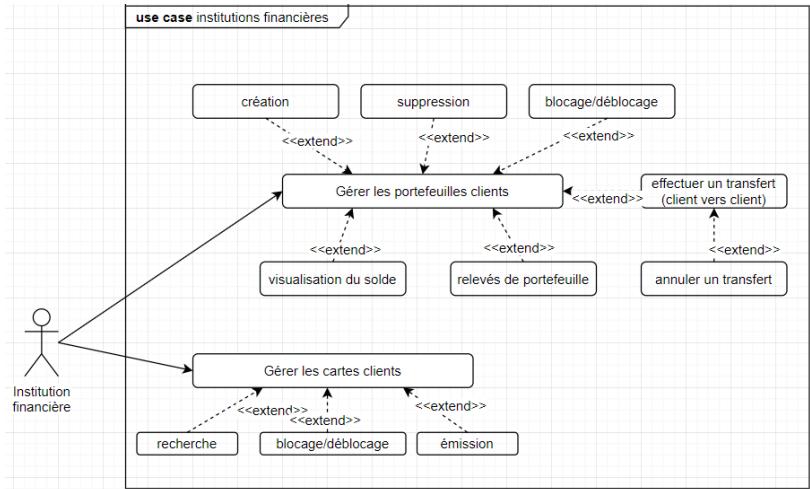


Figure 27 : Use case institutions financières

IX.2.3.1 Cas numéro 1

L'institution financière doit pouvoir gérer les portefeuilles clients (particuliers ou commerçants) (création, modification, suppression, restaurer, bloquer/débloquer, validation, édition de relevés de transactions)

Description détaillée

Résumé : Ce CU décrit la gestion des portefeuilles clients par les banques

Acteurs : Client Web ou Administrateurs

Précondition : Avoir une habilitation

Post condition : gestion d'un ou plusieurs portefeuilles client

Déroulement normal :

La banque choisie un client et modifie, crée, supprime, valide, bloque/débloque son portefeuille.

Le cas d'utilisation est terminé

PAGE DE GESTION D'UN CLIENT EN PARTICULIER

Email	Nom	Prenom	Role	Status
[REDACTED]	Fernando	Amo	Particulier	Validé
[REDACTED]	Macarinelli	Chloé	Admin	Validé
[REDACTED]	Durant	Lola	Banque	Validé
[REDACTED]	FerMacca	chloé	Commerçant	Validé

Client en détail:

Email	Adresse
Nom: Fernando	Ville
Prenom: Amo	Code Postal
Cette	Situation Famille
Profession	Tel

Informations sur un client en particulier

Liste des clients



IX.2.3.2 Cas numéro 2

L'institution financière doit pouvoir demander une habilitation à la BRH afin d'être reconnue comme banque.

Description détaillée

Résumé : Ce CU décrit la fonction de demande d'habilitation d'une banque vers la BRH

Acteurs : Client Web ou Administrateurs

Précondition : aucune

Post condition : habilitation pour tenir un compte institution financière

Déroulement normal :

La banque remplit le formulaire de demande. La BRH valide les documents envoyés et accorde l'habilitation sinon elle refuse.

Le cas d'utilisation est terminé

Demande d'habilitation

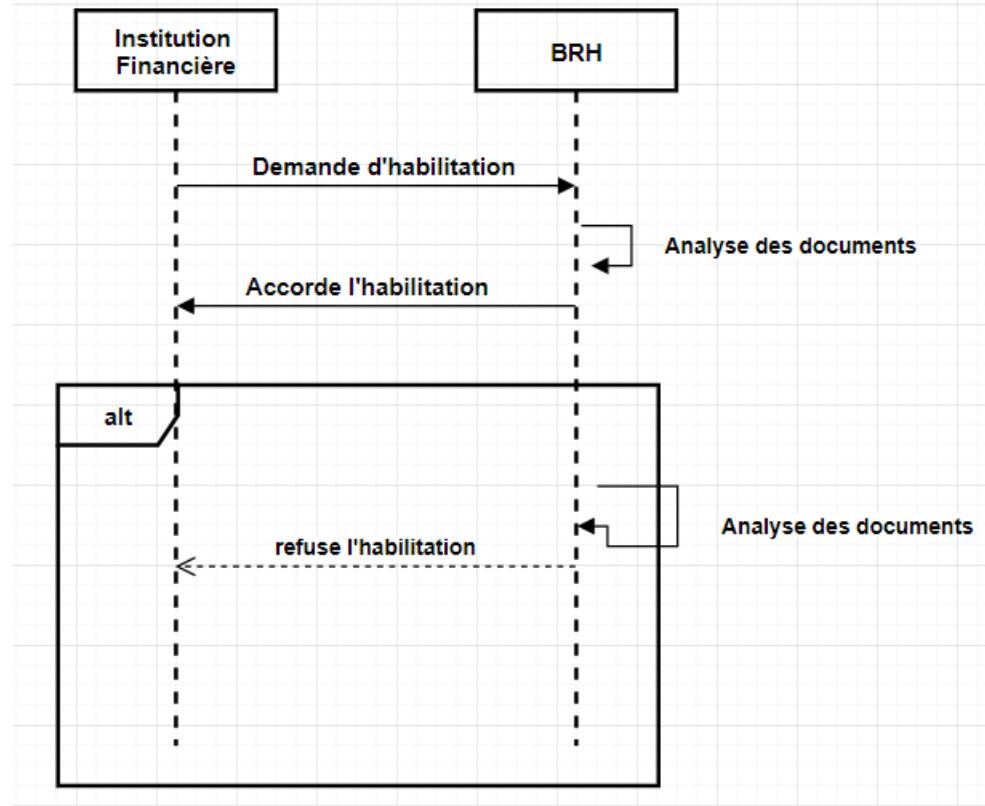


Figure 28 : Diagramme de séquence demande d'habilitation

FORMULAIRE DE DEMANDE D'HABILITATION

The screenshot shows a web-based form titled 'Demande d'habilitation' (Authorization Request). The form is set against a background featuring the BRI logo and a blurred image of a person. The fields required for the application are listed:

- Nom *
- Prenom *
- Nom de la banque *
- Email *
- Mot de passe *
- Confirmer mot de passe *
- Téléphone *

Below the fields are three green buttons for file attachments:

- Joindre votre carte identité
- Joindre votre attestation algéria
- Joindre un justificatif de domicile

At the bottom right of the form are two buttons: 'Enregister' (Register) and 'Annuler' (Cancel).

IX.2.4 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. En plus de ces actions, la BRH peut générer des fonds et accorder ou non des habilitations aux banques.

IX.2.4.1 Cas numéro 1

La BRH doit pouvoir accorder ou non des habilitations aux banques qui en font la demande.

Description détaillée

Résumé : Ce CU décrit la gestion des habilitations par la BRH

Acteurs : Client Web ou Administrateurs

Précondition : Être administrateur de la BRH

Post condition : Validation d'une habilitation

Déroulement normal :

La BRH réceptionne les documents envoyés par une institution financière, les valide ou non.

Le cas d'utilisation est terminé

PAGE DE GESTIONS DES HABILITATIONS (A VALIDER ET DEJA VALIDEES)

*IX.2.4.2 Cas numéro 2*

La BRH doit pouvoir créer de la monnaie.

Description détaillée

Résumé : Ce CU décrit la gestion des portefeuilles clients par les banques

Acteurs : Client Web ou Administrateurs

Précondition : Avoir une habilitation

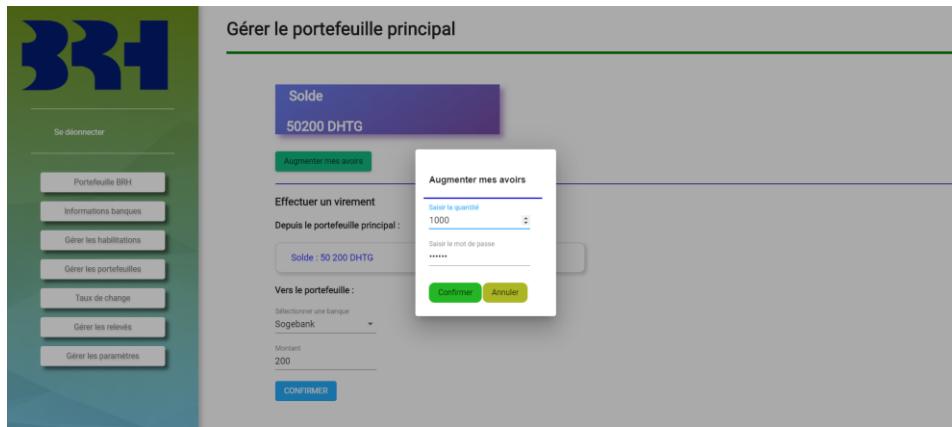
Post condition : gestion d'un ou plusieurs portefeuilles client

Déroulement normal :

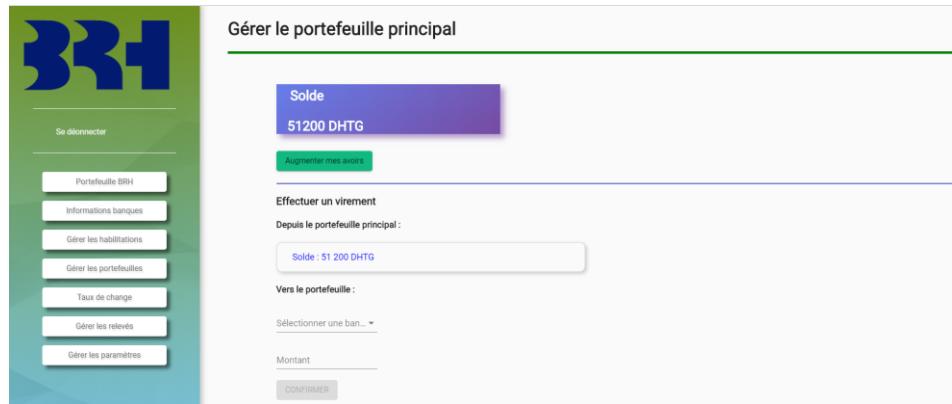
La banque choisie un client et modifie, crée, supprime, valide, bloque/débloque son portefeuille.

Le cas d'utilisation est terminé

CREATION DE DHTG



SOLDE CREDITE DE 1000 DHTG



X. Exigences non-fonctionnelles

X.1 Utilisabilité

- Fonctionnalités accessibles au client Web et au client mobile
- L'application doit être accessible de n'importe quel support
- L'application doit être accessible par plusieurs utilisateurs à la fois
- La création d'une transaction doit pouvoir se faire en 3 clics
- La création d'un portefeuille doit pouvoir se faire en 3 clics

X.2 Performances

- La blockchain doit être capables de valider plus de 1000 transactions par /s
- L'application web se doit d'être capable de présenter les résultats à au moins 1000 utilisateurs simultanément.
- La blockchain doit être à faible consommation énergétique.
- Permettre la validation presqu'instantanée des transactions et à faible coût

X.3 Robustesse

- Accès Internet : disponibilité 24H/24H
- Les informations métier doivent disponibles pendant au moins 10 ans, sans aucune perte

X.4 Sécurité

- Une transaction ne peut être validée sans la signature du client possédant la clé privée
- Aucune modification ne peut se faire que par l'administrateur
- Les mots de passe doivent être cryptées

X.5 Maintenabilité, évolutivité

- Facilité de déploiement
- Application appelée à évoluer sur 10 ans

XI. Architectures

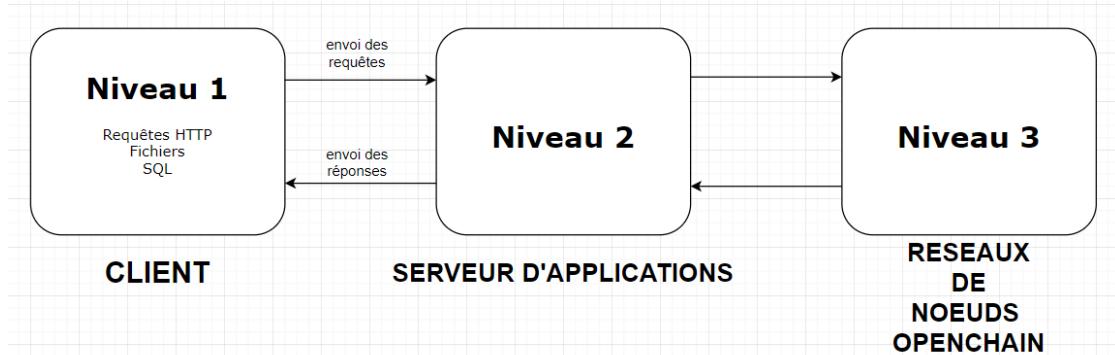


Figure 29 : Architecture générale de l'application

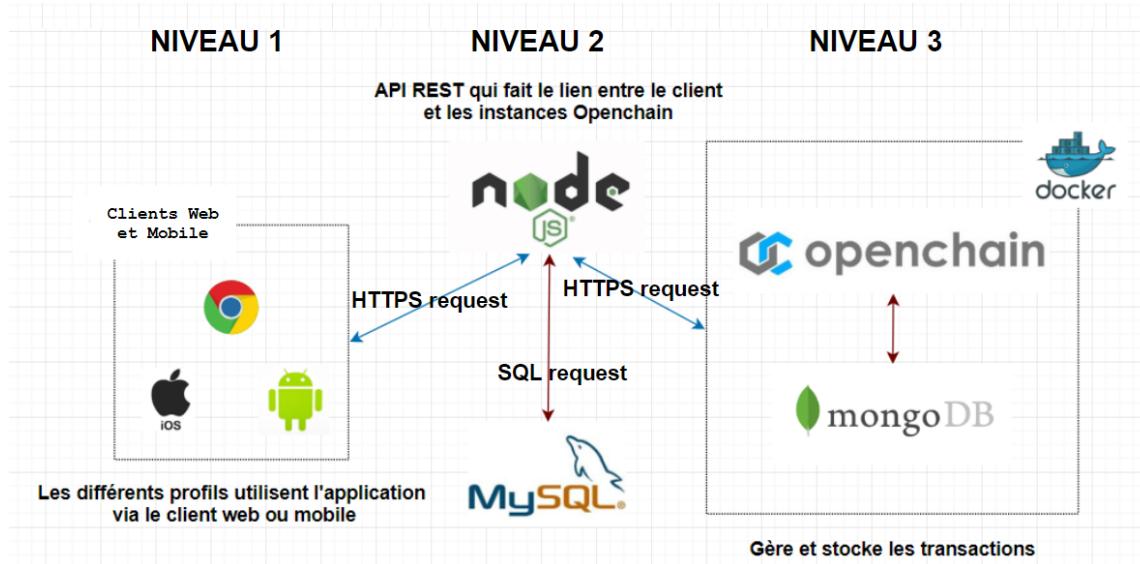


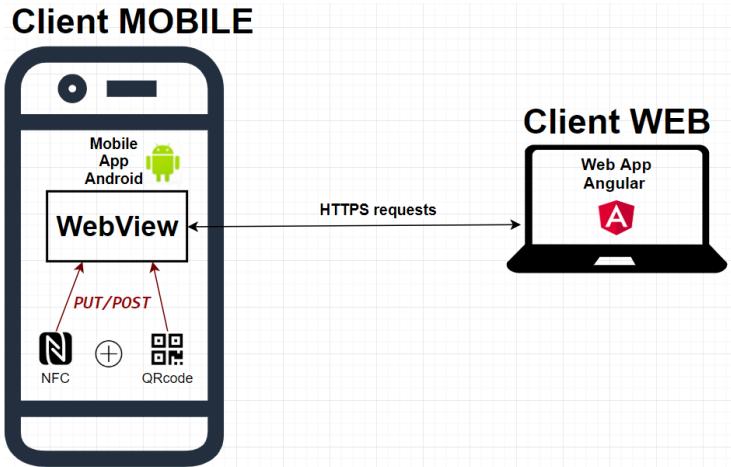
Figure 30 : Architecture technique générale de l'application

XI.1 Niveau 1

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.

L'application mobile sera identique à l'application Web avec comme spécificité d'accéder à la caméra pour lecture de QR code ou utilisation de NFC.

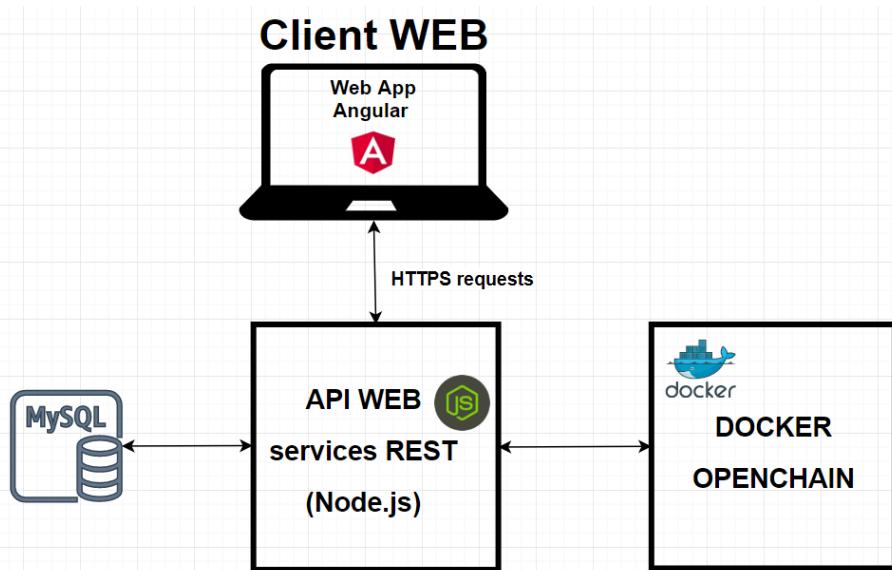
DETAILS DE L'ARCHITECTURE

*Figure 31: Architecture client*

XI.2 Niveau 2

Le client web communique 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)

DETAILS DE L'ARCHITECTURE

*Figure 32: Architecture serveur*

XI.3 Niveau 3

Finalement, l'instance Openchain qui gère les transactions de la blockchain est hébergée dans un conteneur Docker avec une base de données MongoDB où seront stocker les données liées aux transactions.

Avantages de la conteneurisation :

- L'application est isolée
- Possibilité de création d'un réseau de containers
- Léger
- Lancement de l'application simplifié

DETAILS DE L'ARCHITECTURE

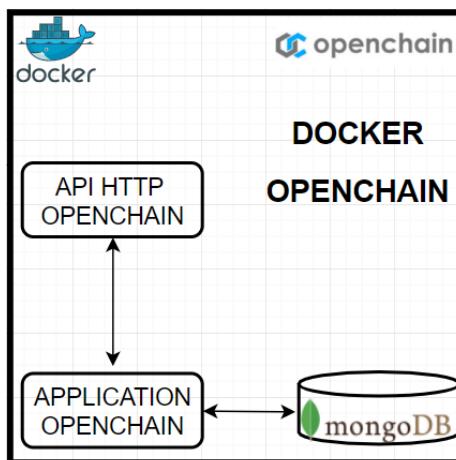


Figure 33 : Architecture Docker Openchain

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.

Client MOBILE

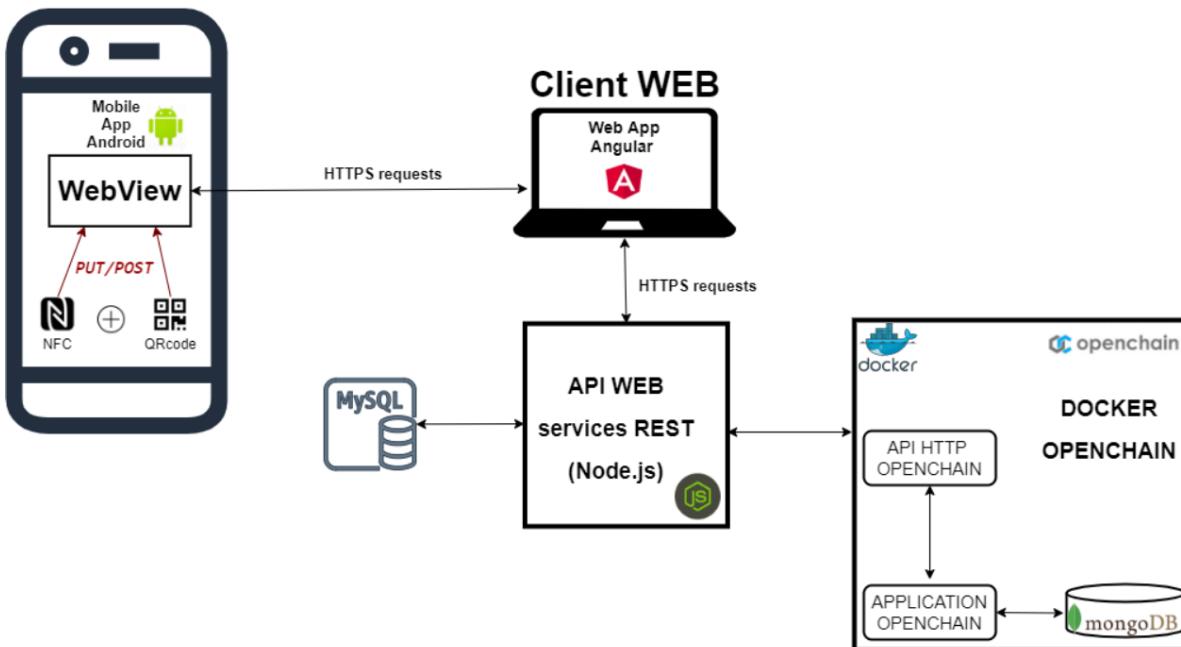


Figure 34 : Architecture complète

XII. Les Améliorations

XII.1 Client Web

L’application web étant presque déjà totalement fonctionnelle, nous avons effectué des modifications surtout au niveau design.

- Responsivité
- Design
- Revue de certaines fonctionnalités

XII.2 Client mobile

Actuellement l’application est accessible uniquement sur PC. Notre objectif est ici de pouvoir l’utiliser sur mobile afin de respecter le cas d’utilisation «[payer un commerçant via l’application mobile \(QR code\)](#)».

Comme étudié dans l’architecture logicielle plus haut, nous nous contenterons à ce stade, de créer une application Android native, qui fera un lien vers l’application web (responsive) et intégrera uniquement la fonctionnalité native de lire un QR code (et lecture NFC).

XIII. Déploiement

Pour la mise en production d'Openchain il est recommandé d'utiliser un serveur proxy tel que Nginx. Cela va permettre plusieurs choses :

- Exposer Openchain via SSL / TLS ⁽²⁾
- Héberger plusieurs instances de serveur Openchain sur le même port
- Modifier le chemin d'URL sous lequel le serveur Openchain est exposé
- Acheminer les demandes vers différentes instances d'Openchain

Dans l'hypothèse où chaque institution gère une partie de la blockchain, et en se basant sur la structure de notre projet, on peut proposer le déploiement suivant :

- Différentes instances validateurs et observateurs de Openchain déployées sur les serveurs, d'une part de la BRH mais également des différentes banques appartenant au réseau. On peut également imaginer déployer des instances sur des serveurs à l'étranger pour plus de sécurité.
- L'application web sur un serveur web
- Le serveur Node sur un serveur différent de celui de l'application web

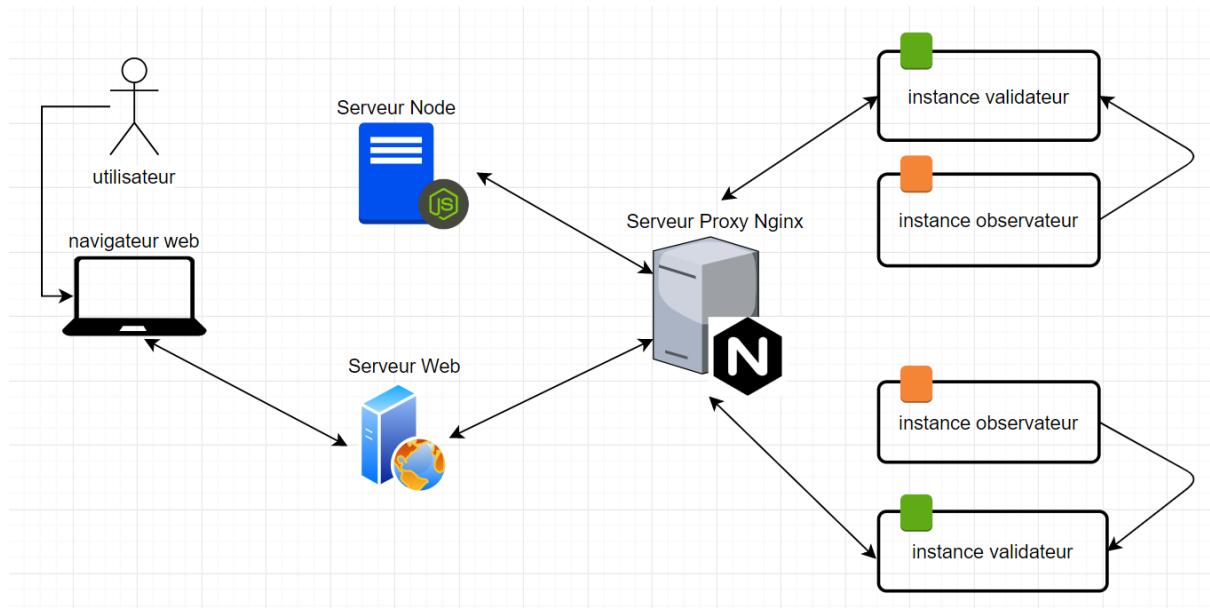


Figure 35 : Déploiement

(2) Transport Layer Security (TLS) ou Sécurité de la couche de transport, et son prédecesseur Secure Sockets Layer (SSL), sont des protocoles de sécurisation des échanges sur Internet.

XIV. Perspectives

XIV.2 Client Web et mobile

Afin d'optimiser au mieux le temps de développement de la solution, ainsi que le coût de développement, nous avons pensé utiliser le Framework « Flutter » qui nous permet de développer une seule application qui sera utilisable sur tous les supports (Client Web, mobile, tablette, ...).

XIV.2.1 Framework Flutter

Flutter, est un Framework open source développé par Google qui a pour objectif de rassembler les points fort de nombreux outils existants. Flutter se fait connaître pour sa capacité à concevoir des applications natives multiplateforme (Android, IOS, Windows, Mac, Linux).

XIV.2.2 Langage Dart

Ce langage « oublié » a comme principale avantage d'offrir deux modes de fonctionnement

- AOT (Ahead Of Time)
- JIT (Just In Time)

XIV.2.2.1 AOT

Dart permet de générer une application native pour chaque plateforme. Le code est donc optimisé pour l'architecture sur laquelle il fonctionne.

XIV.2.2.2 JIT

Dart propose la fonctionnalité de Hot Reload qui permet de réduire considérablement le temps de développement. En effet, le principe de Hot Reload est de réduire le temps entre chaque build, qui est relativement long quand l'on développe une application Android native. On passe donc à quelques millisecondes (pire des cas) entre chaque build.

De plus Dart est performant pour gérer les allocations mémoire et le « Garbage collector ».

XV. Conclusion

Ce projet nous a permis de découvrir une partie de la technologie blockchain dont nous n'avions pas forcément connaissance.

Il a permis à certains d'entre nous d'appréhender les difficultés d'intégrer un projet de développement en cour de route, ainsi que l'organisation et gestion de projet avec des collaborateurs n'étant pas présent à temps plein.

L'objectif principal du projet était de créer un prototype de cryptomonnaie sociale permettant aux gens non bancarisés de l'être. Mais également de réduire les coûts de création de monnaie.

L'état actuel de l'application est suffisant pour en faire un Proof Of Concept, cependant il est envisageable d'agrandir l'infrastructure à plus grande échelle (domaines distincts par banques) pour mieux refléter la réalité.

XVI. Webographie et Bibliographie

- <https://blockchainfrance.net> , Blockchain France
- <https://docs.openchain.org/> , documentation OpenChain
- <https://hyperledger-fabric.readthedocs.io/> , documentation Hyperledger Fabric
- <https://flutter.dev/> , site web officiel de Flutter
- Rapports et travaux réalisés par IBEGHOUCHENE Nadir, SAAD MEHDI, Sergio Simonian, Luke Bancroft-Richardson, année 2018-2019, disponibles sur :
https://freedcamp.com/MBDS_6di/Projet_DIGITAL_G_LzG/todos
- Document Excel de simulation de budget réalisé par Mr GAL, disponible sur :
https://www.dropbox.com/home/EtuMasterMBDS2019/2020/9supports_de_cours/GAL_Project_sheets?preview=24-TD1-Preparation.xlsx