IUT Nancy Charlemagne, 2021 - 2022

Porte-monnaie virtuel

-

Rapport de projet tutoré

Tuteur : Pierre André Guénégo

Membres :

- Antoine Chevaleyre
- Lucas Cordurié
- Michel Grolet
- Gabin Hemmerle
- Julien Sacquard

Table des matières

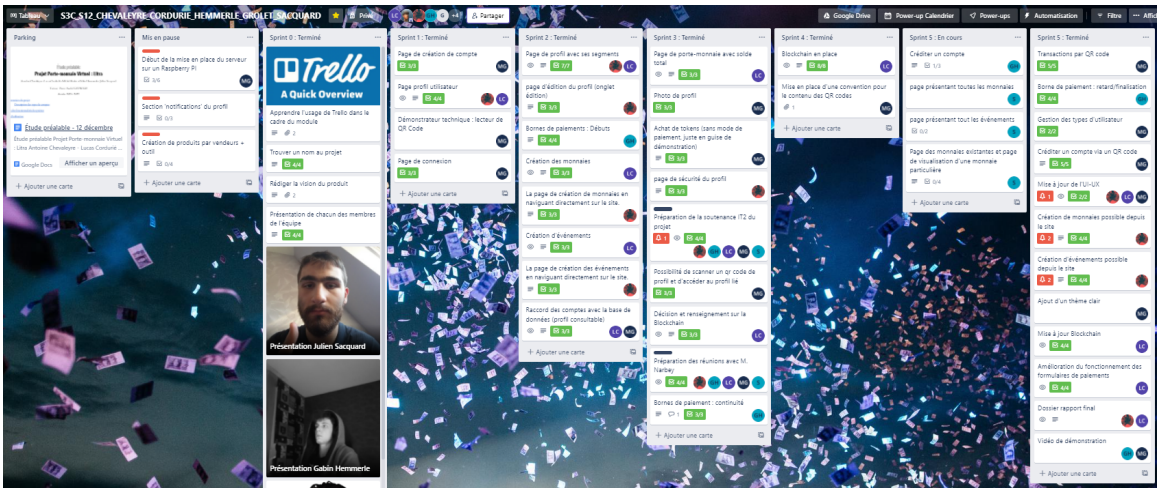
1. Introduction

Ce document a pour objet d'exposer un rapport de projet tutoré portant sur le sujet du porte-monnaie virtuel. Nous avons choisi de nommer notre projet *Litra*, le but est de développer une application web permettant aux utilisateurs de réaliser des transactions via des monnaies virtuelles. Le projet est destiné à des festivals ou des conventions ayant besoin d'un moyen de paiement non fiduciaire. L'application permettra de réaliser des transactions via QR code et carte RFID.

Pour réaliser ce projet, une équipe a été formée, composée de Antoine Chevaleyre, Lucas Cordurié, Michel Grolet, Gabin Hemmerle et Julien Sacquard. Chacun s'est occupé d'une partie différente du projet, Gabin s'est concentré sur la partie paiement via carte RFID, le reste de l'équipe s'est occupé de réaliser l'application web. Lucas a notamment réalisé une Blockchain, Michel a mis en place un scanner de QR Code et a développé la création de comptes, Antoine s'est chargé de la mise en place des formulaires et des raccords avec la base de données et Julien de la création de la base de données.

Le projet s'est déroulé du mois d'octobre 2021 jusqu'au mois d'avril 2022 avec en premier temps une analyse préalable de notre projet puis, dans un second temps, la partie développement. Le projet a été entrecoupé par 2 soutenances avec nos accompagnateurs de projet tutoré, M. Narbey et M. Guénégo, ainsi que 3 rendez-vous avec M. Narbey au fil de nos itérations.

Le planning divisant les tâches en itérations se composait de 8 parties. Suite à des retards pris dans le travail en début de projet, un nouveau planning en 6 itérations de 2 semaines chacune a été réalisé. Ce dernier a été tenu et est resté d'actualité. Nous avons mis sur Trello le découpage des tâches à mesure de nos avancements. Les deux dernières itérations ont toutefois été fusionnées dans la mesure où la 6ème était principalement une phase de débogage et d'amélioration esthétique.



2. Analyse

a. Description détaillée du sujet

L'objectif du projet est de créer une solution de paiement, accessible en ligne, dans le but de remplacer les devises FIAT par une monnaie virtuelle dans le cadre d'événements. Cette idée de remplacer de la monnaie réelle par des tokens est déjà présente dans des salles de jeux avec des bornes d'arcade où on utilise des jetons en plastique à la place de pièces de monnaie. Ici, le but serait de l'utiliser pour de l'événementiel dans des festivals, expositions ou encore conventions.

Pour mettre en place cette solution, nous avons réalisé une application web. Un utilisateur peut créer un compte sur le site pour ensuite accéder à un tableau de bord sur l'onglet profil. L'utilisateur peut consulter les différents événements qui ont été publiés et se procurer le token propre à l'événement via le site. Il peut également consulter son porte-monnaie, voir son QR code, utiliser le scanner, effectuer des transactions et modifier les informations de son profil (mot de passe, adresse mail, numéro de téléphone...).

Via le tableau de bord, un utilisateur qui aurait le rôle d'organisateur peut publier des événements et des monnaies et peut par la suite les consulter.

Un utilisateur ayant le rôle de vendeur peut générer des QR Codes pour effectuer des transactions.

- Application web :
    - Page d'inscription / de connexion
    - Page des événements
    - Page des monnaies
    - Page de scanner
    - Page du portefeuille
    - Page de paiement
    - Tableau de bord (Profil)
        - QR code
        - recharger (obtenir des tokens)
        - changer mes droits (démonstration pratique)
        - voir les événements dont vous êtes le créateur
        - voir les monnaies dont vous êtes le créateur
        - éditer le profil
        - sécurité (changer de mot de passe)

        - se déconnecter
- Transfert de monnaies par :
    - QR code
    - RFID
    - ID utilisateurs
- Un terminal de paiement avec puce RFID :
    - Arduino wifi
    - Boîtier m5stack

b. Découpage fonctionnel du projet

Chacune des parties suivantes du projet peut-être considérée de façon individuelle et entraîne son propre résultat. Certaines ont été réalisées en parallèle, d'autres en simultané.

1. Mise en place et mises à jour de la base de données

2. Développement du site web en front-end (HTML, CSS, Javascript)
    - Maquettage
    - Création de la charte graphique
    - Fonctions JS pour l'expérience utilisateur

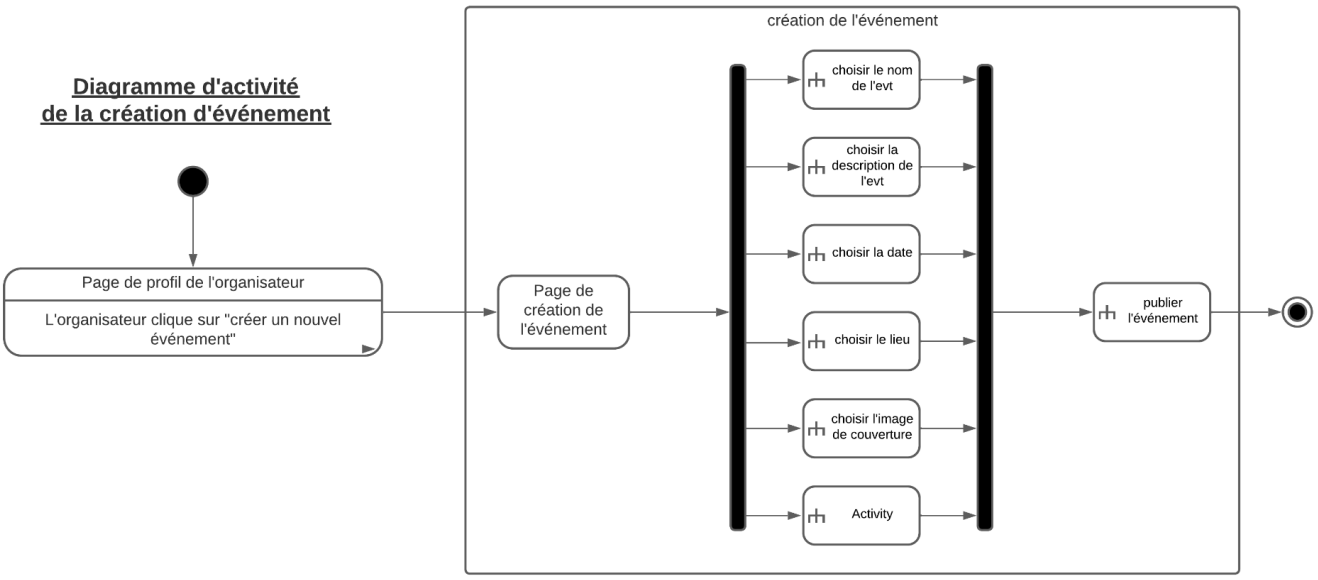
3. Développement du site web en back-end (PHP, Laravel, Eloquent)
    - Mise en place et redéfinitions des routes
    - Récupérations de données via Eloquent
    - Implémentation de fonctionnalités à travers le modèle MVC

4. Développement et mise en place de la Blockchain et de ses outils

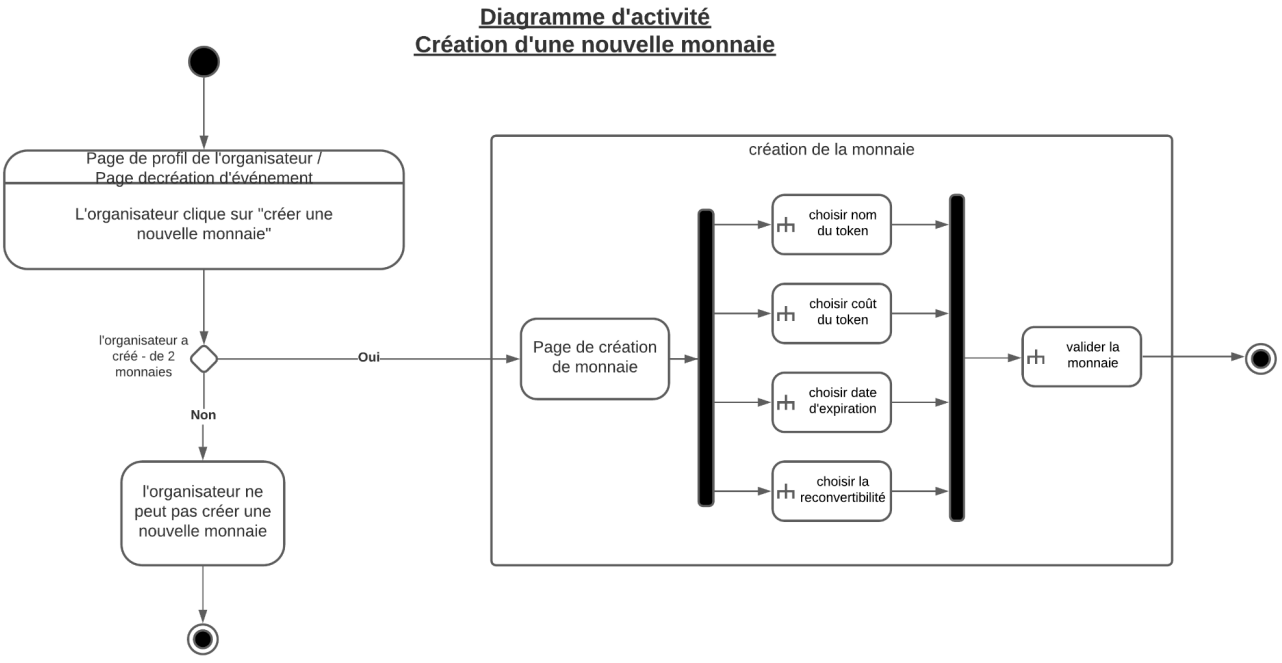
5. Développement et mise en place de la lecture par RFID

Fonctionnalités principales

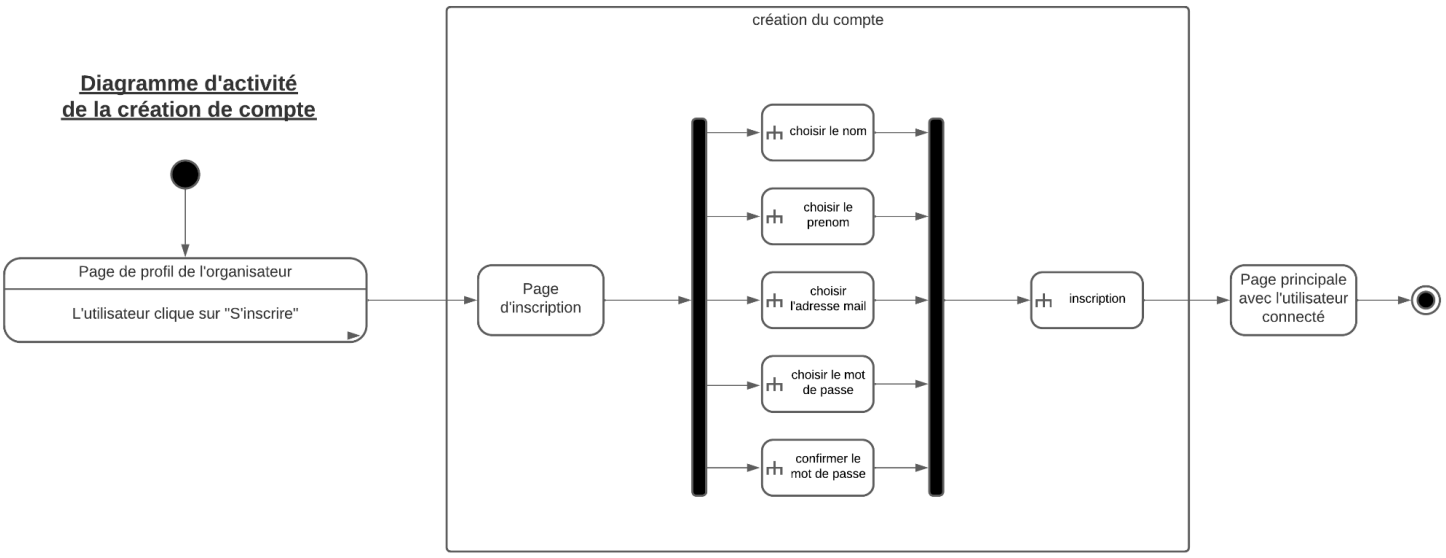
1. Création d’événements



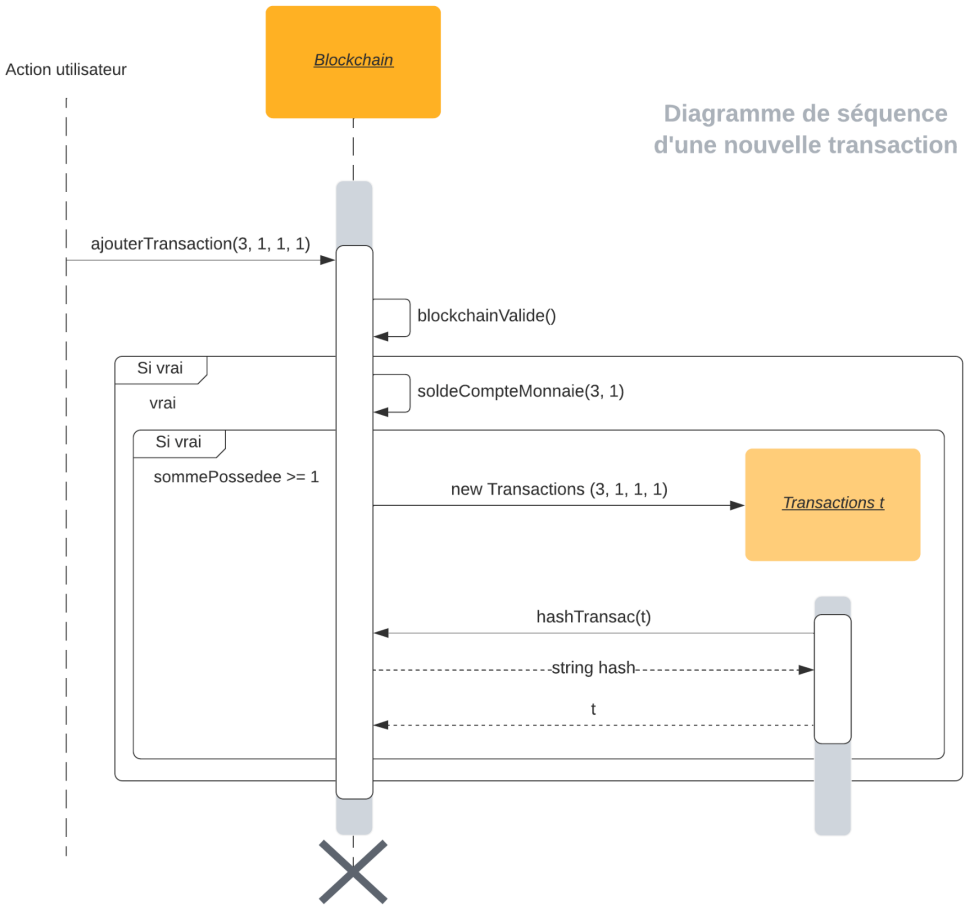
2. Création de monnaies



3. Création de compte



4. Effectuer des transactions



c. Modèles UML utilisés

Nous avons pu mettre certains de nos travaux sous forme de diagrammes UML, les modèles ayant été utilisés étant :

- Diagramme de classe / de structure de base de données
- Diagramme de cas d'utilisations
- Diagramme de séquence système
- Diagramme d'activité
- Diagramme d'état
- Diagramme User / Si

Diagramme de cas d'utilisation de Litra :

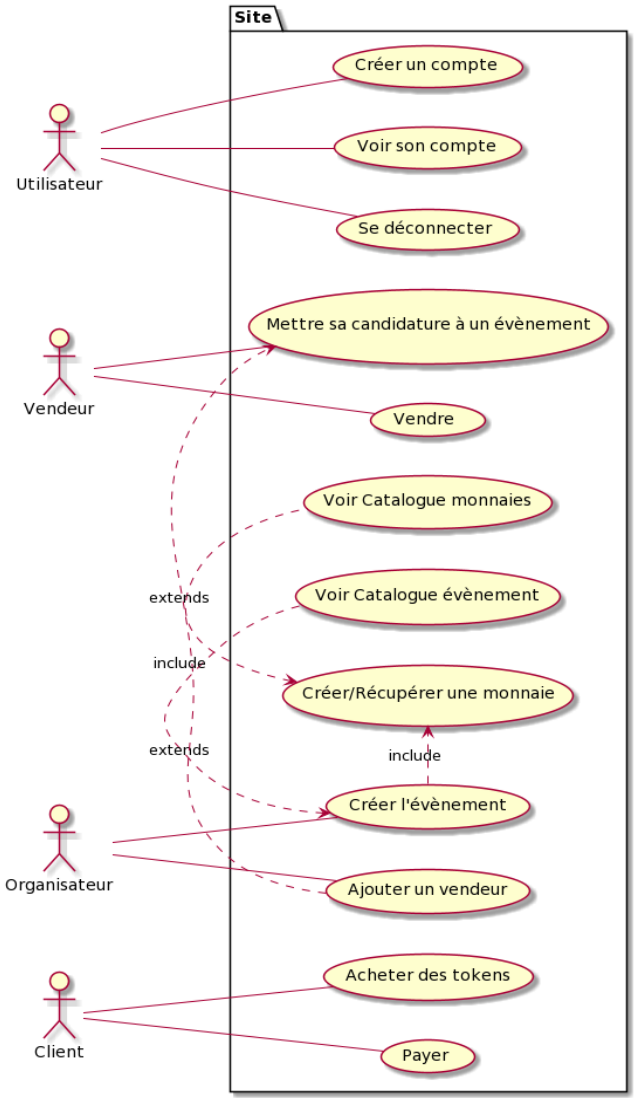
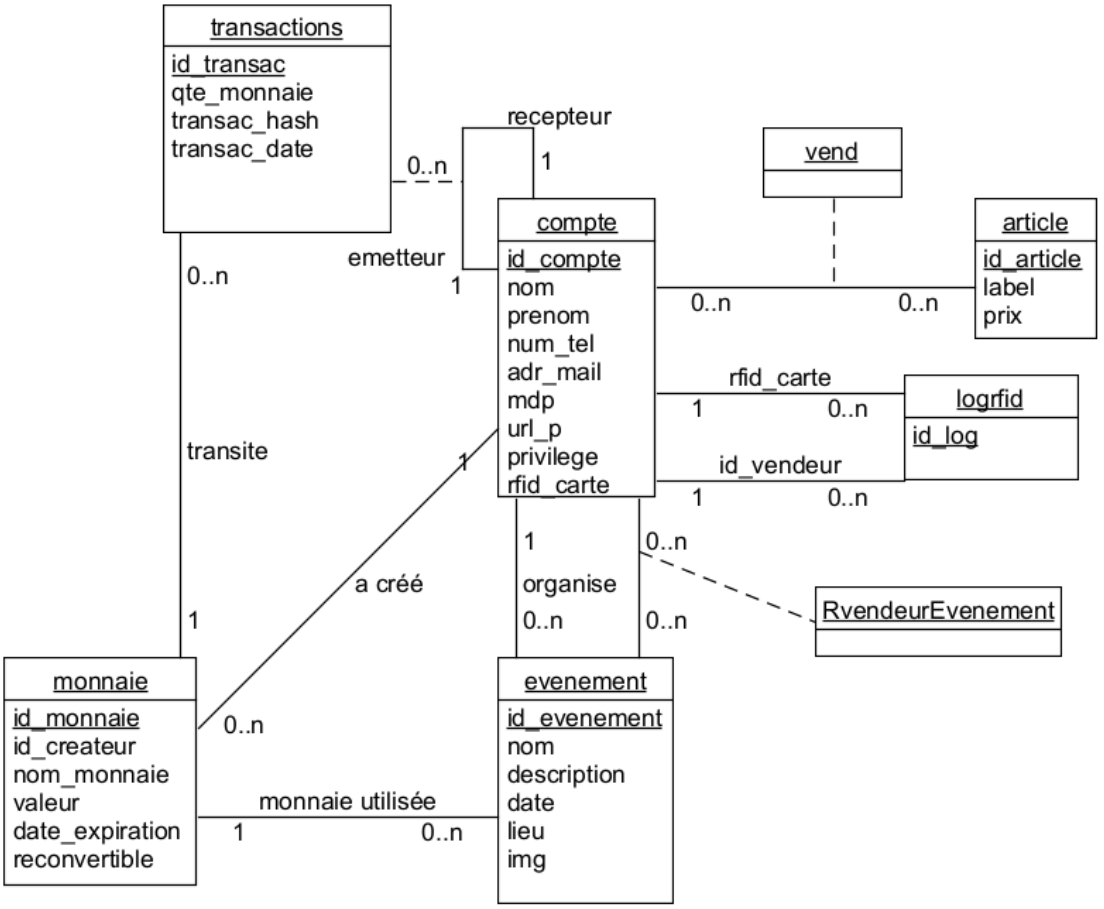


Diagramme final de la base de données :



d. Évolution du projet

Au début du projet, notre réflexion et nos plans se sont constitués autour d'une idée large, que nous avons tenté de développer largement afin d'avoir une multitude de travaux à réaliser.
L'objectif dès le début n'était pas de tout finaliser, même si cette option constituait un idéal enviable.

Au cours de notre avancée, nous avons donc reporté et/ou abandonné des points de nos plans initiaux afin de mieux préciser notre projet, et plus précisément, ce que nous souhaitions réaliser dans les temps impartis.

Ainsi, nous avions initialement prévu de programmer notre site en PHP avant de le refaire en Node.js pour le résultat final.
Par souci de simplicité, nous avons donc commencé le développement en PHP, tout en suivant un cours de Node.js en parallèle.

Le retard pris sur certaines fonctionnalités et le caractère dispensable d'un site en Node nous ont amené à abandonner cette idée.

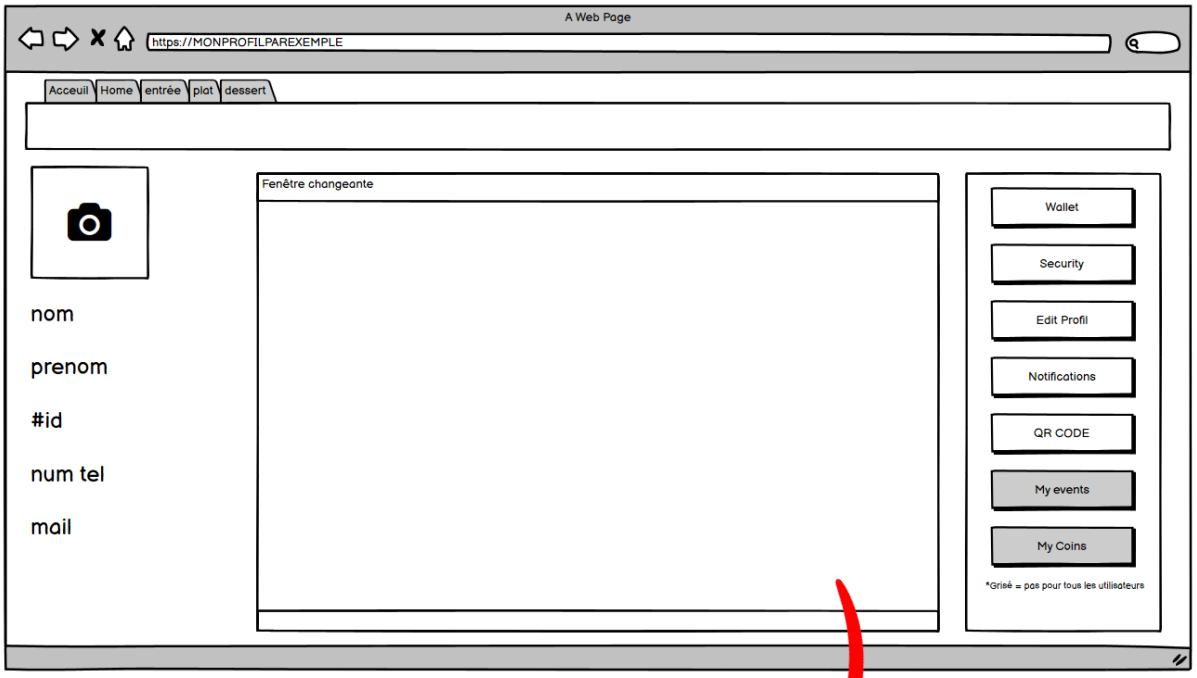
Certaines fonctionnalités ont également été mises de côté avec la prise de retard. On pourra citer le système de messagerie que nous avions prévu sous le nom "notifications", permettant entre autres d'envoyer des demandes d'un utilisateur à un autre.

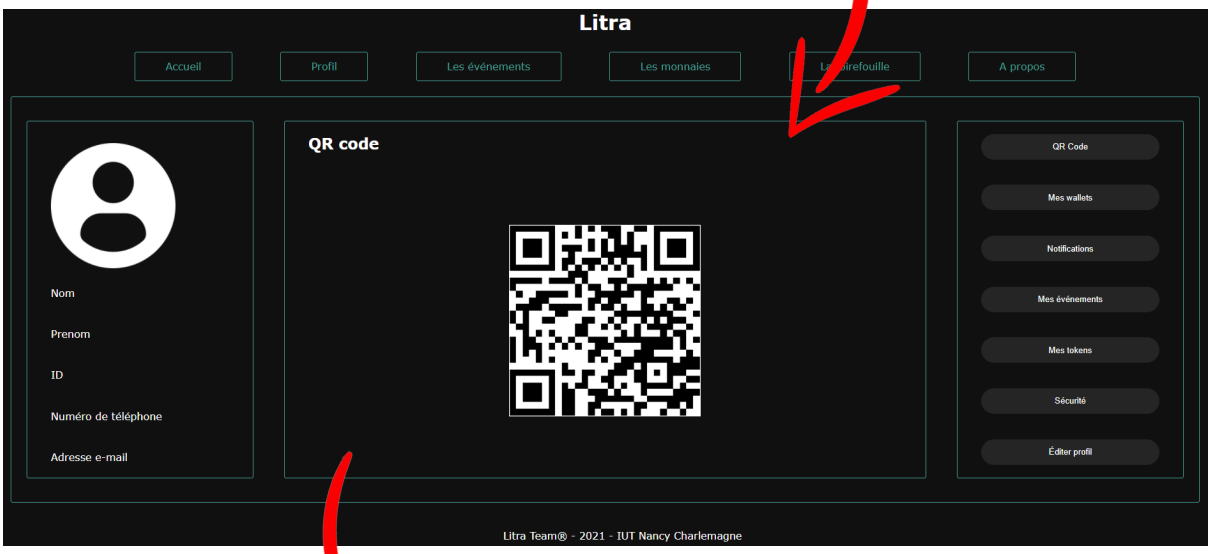
Demander à changer le niveau privilège de son compte, rejoindre un événement en tant que vendeur, demandes ou réclamations aux administrateurs, ces fonctionnalités découlant de la messagerie ont été suspendues. Le changement de privilège est toutefois possible sous forme de démonstration sur le site.

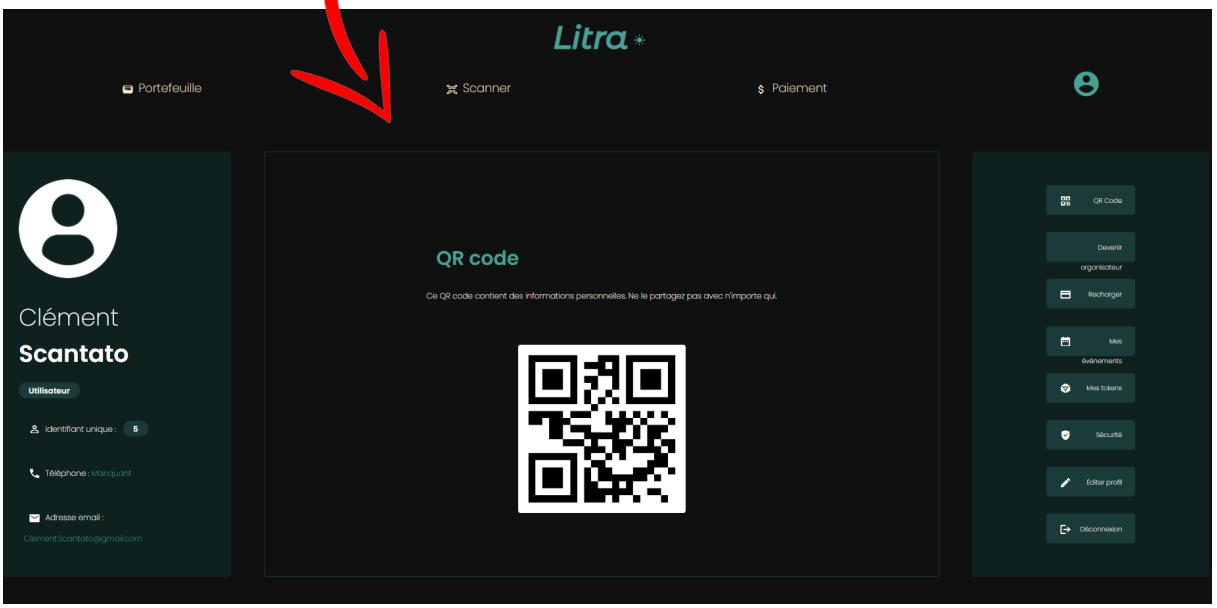
Dans le même esprit, la double authentification et l'outil pour les vendeurs (enregistrement de produits et création de paniers) ont été repoussés et ne seront pas réalisés durant cette dernière itération.

Aussi, notre système s'étant clairement orienté vers un fonctionnement en ligne durant le développement, la mise en place d'un serveur local a été abandonnée.
Avec plus de temps, cet aspect aurait été exploré puisqu'il reste intéressant dans notre schéma de fonctionnement.
La lecture RFID a, quant à elle, été développée comme prévu.

L'architecture de notre site, le placement de certaines pages et leurs visuels ont également connu des changements visant à simplifier l'expérience utilisateur.


A Web Page
https://MONPROFILPAREXEMPLE
Acceuil
Home
entrée
plat
dessert
Fenêtre changeante
nom
prenom
#id
num tel
mail
Wallet
Security
Edit Profil
Notifications
QR CODE
My events
My Coins
*Grisé = pas pour tous les utilisateurs

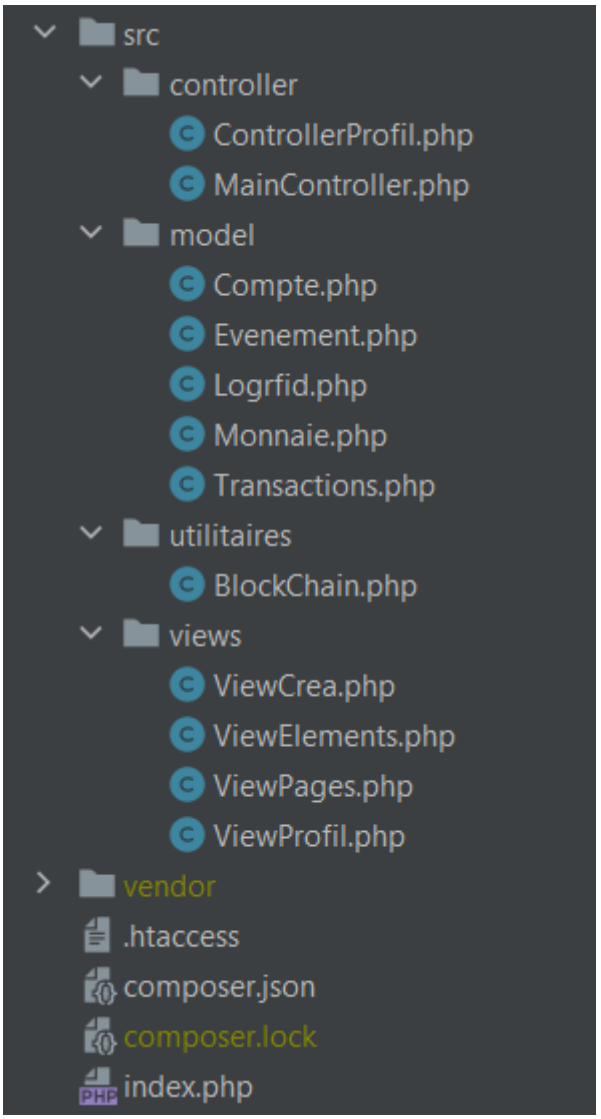

Litra
Accueil
Profil
Les événements
Les monnaies
A propos
QR code
Nom
Prenom
ID
Numéro de téléphone
Adresse e-mail
QR Code
Mes wallets
Notifications
Mes événements
Mes tokens
Sécurité
Éditer profil
Litra Team® - 2021 - IUT Nancy Charlemagne


Litra
Portefeuille
Scanner
Paiement
Clément
Scantato
Utilisateur
Identifiant unique : 5
Téléphone : Manquant
Adresse email :
ClementScantato@gmail.com
QR code
Ce QR code contient des informations personnelles. Ne le partagez pas avec n'importe qui.
QR Code
Devenir organisateur
Recharger
Mes événements
Mes tokens
Sécurité
Editer profil
Déconnexion

3. Réalisation

a. Architecture du projet

Le projet s'est structuré sur le modèle d'une architecture MVC. On retrouve donc, de fait, 3 parties majeures.



Les modèles permettent de faire le lien avec les tables de la base de données. Des correspondances peuvent être établies entre plusieurs modèles, permettant par exemple à l'aide d'une fonction d'utiliser une table de jonction sans en faire le modèle (BelongsToMany).
On peut ensuite faire des requêtes Eloquent en partant de ces modèles.
Les contrôleurs seront l'emplacement privilégié de ces requêtes.

Les contrôleurs permettent d'afficher les vues, mais aussi de traiter leurs formulaires en récupérant les informations entrées dans les différents champs puis, d'envoyer les créations et modifications vers la base de données. Cette partie a été séparée en deux, ControllerProfil contrôlant le profil et MainController les fonctionnalités principales de l'application comme la création d'événement et de monnaies ou encore des transactions.

Les vues se concentrent sur l'affichage, avec principalement le code HTML, mais aussi la récupération des données de la base pour l'affichage des événements, des informations du compte, etc. Elles ont été divisées selon leur utilisation, ViewProfil pour les pages du profil, ViewElements pour les éléments comme la barre de navigation du site, ViewPages pour les pages en général et ViewCrea se concentre sur les pages comprenant les formulaires de création de monnaie et d'événements.

Voilà pour le MVC, il reste toutefois quelques éléments distincts.

L’index s’occupe de réaliser la connexion entre notre projet et notre base de données, il détermine également le comportement de l’application grâce aux routes GET et POST, associe l’URL attendue à chaque page et précise quelle méthode de quel contrôleur va s’effectuer sur chaque page.

Finalement, une classe Blockchain a été réalisée distinctement des autres afin que le code relatif à celle-ci ne soit pas mélangé avec le reste. Les fonctions qui composent cette classe sont donc utilisables dans les vues et contrôleurs.

b. Tests de validation

Afin de vérifier que le cœur de notre application fonctionne conformément à nos attentes, une certaine somme de tests est à prévoir.

Le premier est évidemment que la base de données se mette en place sans problème, sans quoi, peu de choses se dérouleront comme prévu.

L’inscription et la connexion sur le site doivent être possibles et insérer bel et bien le nouveau compte dans la base de données. Le hachage du mot de passe ne doit pas être un obstacle à la connexion.

L’accès au profil, affichant les informations du compte, doit être possible et en place. L’affichage doit être adapté au privilège du compte et permettre certaines fonctionnalités réservées à ces niveaux de privilèges.

La modification de quelques informations telles que le mot de passe ou le numéro de téléphone est possible via le profil.

La création d’événement et de monnaies est possible aux comptes autorisés, les insertions se font bien et les créations se retrouvent dans les pages prévues.

La navigation ne doit pas amener à une quelconque erreur et doit permettre en premier lieu de consulter les événements existants ainsi que les monnaies associées.

On peut acheter une monnaie et recevoir la somme sur son solde (“Wallet”).
Il est possible d’envoyer cette monnaie à un autre compte dans la limite de la quantité possédée.
On pourra aussi, avec les bons niveaux de privilèges, créer des QR Codes de demandes de paiement qui, lorsqu’ils seront scannés, permettront de virer la

quantité de monnaie du token demandé à la personne ayant émis le QR Code (dans la limite du solde du compte scannant).
Le paiement par RFID fonctionne de la même façon.

Toutes les transactions possibles et autorisées seront insérées dans la base de données et seront consultables sous forme d'un résumé que constitue le Wallet.

Pour s'assurer du bon fonctionnement de la Blockchain, on pourra l'altérer volontairement depuis l'interface de la base de données (PhpMyAdmin dans notre cas), et visualiser l'erreur sur le site.
La notification de la corruption est visible dans plusieurs pages faisant usage de la Blockchain et de ses fonctionnalités, comme le Wallet par exemple.
On doit pouvoir consulter la corruption si un quelconque champ est changé dans n'importe quelle ligne de la table des transactions.
Le message informant de la corruption est visible dès que celle-ci a eu lieu, après rafraichissement de la page si nécessaire.

c. Difficultés rencontrées

Tout d'abord, lors de l'étude préalable, il a été difficile de s'accorder sur la finalité du projet et sur le fonctionnement de ses fonctionnalités. Un exemple à prendre serait le scan de QR code, savoir si l'utilisateur fait une transaction en faisant scanner son QR code comme sur l'application Izly ou à l'inverse, que l'utilisateur pouvait faire une transaction en scannant le QR code d'un autre utilisateur comme si l'on scannait des produits à une caisse automatique.
Le problème vient du fait que si un utilisateur peut se faire retirer de l'argent en se faisant scanner son QR Code, et que tous les utilisateurs disposent d'un scanner, il risque d'y avoir des vols. Chose qui n'arriverait pas si on utilisait la méthode inverse pour établir une transaction, à moins de se faire voler son appareil.
Les problèmes d'organisation de ce type ont été moins nombreux avec le temps et les outils fournis.

L'architecture du site a fini par devenir assez importante et il a été difficile de s'y retrouver à un moment. Des modifications ont par la suite eu lieu et ont clarifié la situation, ainsi que l'expérience utilisateur.

La lecture des cartes RFID a constitué une grande difficulté à cause de la lecture qui ne se faisait pas correctement, et ce, malgré un code fonctionnel. Le problème venait du fait que la lecture du contenu de la carte se faisant tellement rapidement à

travers le lecteur que l'affichage de la carte n'avait pas le temps de se faire correctement et cela affichait deux résultats dans le terminal.

```
M5Stack initializing...OK
http://172.20.10.3/test/m5/□§§§§§§§§§§§§
http://172.20.10.3/test/m5/770046CCDC21□§
```

Autrement dit, deux GET étaient effectués et ceux-ci étaient dysfonctionnels à cause des caractères spéciaux comme dans la capture ci-dessous.
Dans la boucle qui scanne les caractères, un "delay" a été ajouté pour laisser le temps à la lecture de se faire correctement même si ce n'est pas la meilleure pratique. Ainsi le problème a été résolu et la lecture est devenue normale.

L'implémentation du paiement par RFID a également constitué une difficulté. Nous avons dû créer une table de logs qui répertorie les cartes scannées associées au vendeur qui les a scannées.

L'implémentation de la librairie de scan de QR codes a été complexe puisqu'il était nécessaire d'apprendre les promesses Javascript alors que nous ne les avions pas encore abordées en cours.

Il y a aussi eu quelques problèmes de priorité sur la priorité des fichiers CSS pour le changement de thème.

La prise en main d'Eloquent était assez rude au démarrage, même si des projets d'autres modules ont pu simplifier la chose.

Enfin, la Blockchain a pu être difficile à appréhender. Les possibilités sont vastes et on a tôt fait de s'y perdre. Après avoir identifié la manière de faire et les fonctionnalités à utiliser, il restait toutefois à réfléchir à un système bien étanche et sécurisé, sans duplicatas d'information, sans appels dupliqués…
Cette entité aura évolué jusqu'à la fin du développement.

Bien sûr, comme souvent dans ce genre de projets, le temps aura été l'un de nos principaux ennemis.

4. Conclusion

Nous arrivons donc à la fin de ce projet et de ce document dans lequel nous avons passé en revue de nombreux points.

Depuis l'étude préalable, notre projet a connu des évolutions, s'est précisé. Initialement, ce sujet du porte-monnaie virtuel nous conduisait vers une installation plus lourde en matériel, précisément centré sur la localité, mais dans son développement, l'aspect service s'est avéré plus intéressant.

Le temps imparti a joué un rôle dans nos choix et a par conséquent modelé le résultat final que nous vous présenterons au cours de cette ultime présentation orale du 8 avril 2022.

Il s'agit d'un travail de longue haleine qui représente des centaines d'heures cumulées. Choix du sujet, réflexion, conception, modélisation, réalisation, présentation…
Les projets de modules sont nombreux au sein du DUT informatique mais aucun ne sollicite autant l'éventail des capacités que nous avons acquises.

Il reste encore beaucoup à faire pour ce projet, des éléments qui, bien que secondaires, peuvent rendre ce projet bien plus abouti qu'il ne l'est actuellement.
Les fonctionnalités abandonnées par faute de temps, comme la double authentification, des fonctionnalités pouvant agrandir le cadre d'utilisation de notre solution, des fonctionnalités auxquelles nous n'avons pas pensé, changeant le confort d'utilisation et la sécurité…
Le cœur de l'application est en revanche bien présent et fonctionnel : comptes, Blockchain, transactions, RFID, QR codes…
Il serait possible de poursuivre nos travaux, nous ne nous y opposerions pas, mais la partie de découverte que représente certaines des fonctionnalités présentes ci-dessus est en majeure partie entamée, ce qui en réduit l'intérêt.

Quoi qu'il en soit, ce projet constitue une expérience de projet en équipe sur le moyen terme que nous n'avons jamais connu auparavant.
Le résultat, bien qu'incomplet à certains égards, reste ce que nous avons pu faire de plus complexe et achevé.

5. Glossaire

RFID : De l'anglais radio frequency identification, soit la radio-identification, permet de mémoriser et récupérer des données à distance par le biais de marqueurs appelés « radio-étiquettes », qui dans notre cas sont des cartes à puce.

QR CODE : Type de code-barres à deux dimensions — format optique lisible par machine pouvant être visualisé sur l'écran d'un appareil mobile ou imprimé sur papier. On l'appelle code à réponse rapide (**Q**uick **R**esponse), il présente un grand intérêt lorsqu'il s'agit de mettre de l'information sous forme visuellement traitable par une machine.

FIAT : Devise traditionnelle, reconnue et utilisée par un État, dont le cours est imposé et réglementé. L'euro et le dollar sont des exemples tout à fait valables de monnaies FIAT.

Token : Il s'agit basiquement d'un jeton. Dans notre cas, c'est le nom que l'on donne à une monnaie qui n'est pas une FIAT, une monnaie fictive / virtuelle.
On pourra employer le terme comme unité d'une monnaie, "un token de telle monnaie".

Wallet : Porte-monnaie / Solde
On y retrouve les monnaies que l'on possède, que l'on nomme ici des Tokens.

Blockchain : Technologie regroupant une somme de procédés reposant sur une architecture particulière.
Dans notre cas, on se limite à un principe de chaîne entre les maillons, nos "transactions", ce qui permet de s'assurer qu'aucune transaction ne disparaît ou ne se retrouve modifiée.
Une fois créée et insérée dans le système (la base de données), l'information est datée et inaltérable, tout du moins, plus rien ne peut être ajouté après cela.

6. Liens vers des ressources supplémentaires

https://github.com/univ-lorraine-iut-charlemagne/S3C_S12_CHEVALEYRE_CORDURIE_HEMMERLE_GROLET_SACQUARD

https://trello.com/b/sTQL1ful/s3cs12chevaleyrecorduriehemmerlegroletsacquard

https://webetu.iutnc.univ-lorraine.fr/www/grolet4u/litra/