



Ecole Nationale
Supérieure
d'Informatique et
d'Analyse Des
Systèmes

ENSIAS, Filière Sécurité des Systèmes d'information

Projet de fin d'année 2ème année

Développement et sécurisation d'une application mobile pour le MPayment



Wallet 1.0

Réalisé par :

Ftaichi Zakaria

El Oufir Hassan

Encadrant/jury :

Mr. Doukkali Abdelaziz

Mme. Elbekkali Hanane

Année universitaire

2019/2020

Remerciements

Au terme de ce travail nous profitons pour exprimer nos vifs remerciements à toute personne ayant contribué dans ce projet de près ou de loin.

Nous exprimons également notre reconnaissance à ceux qui ont fait preuve de disponibilité à chaque fois que nous avons eu besoin de leurs soutiens et pour les conseils qu'ils nous ont prodigué.

Résumé

La possibilité de payer en agitant simplement un téléphone portable près d'un point de vente représente une nouvelle ère de paiement très intéressante. Donc, dans un écosystème où les institutions financières, les opérateurs de réseaux mobiles doivent gérer ce processus de paiement, la sécurité est primordiale.

L'objectif principal du projet fut de réaliser une application mobile de paiement par QR CODE. Le développement de cette application est accompagné par l'implémentation des outils de sécurisation, ainsi l'application propose les fonctionnalités nécessaires d'un portefeuille électronique et assure une utilisation sécurisée, ceci concerne les transactions, les comptes des utilisateurs et leurs confidentialités.

Abstract

The possibility of paying by simply waving a mobile phone near a point of sale represents a very interesting new era of payment. So, in an ecosystem where financial institutions, mobile network operators have to manage this payment process, security is paramount.

The main objective of the project was to create a mobile QR CODE payment application. The development of this application is accompanied by the implementation of security tools, so the application offers the necessary functionalities of an electronic wallet and ensures secure use, this concerns transactions, user accounts, and their confidentiality.

Table des figures

Figure 1 number of non-cash transactions worldwide for north America, Europe, mature APAC, Latin America, emerging Asia and CEMEA.....	12
Figure 2 : Cross-border volume trends	12
Figure 3 :Schéma du processus de la méthode agile SCRUM.....	15
Figure 4 :Croissance globale de projet de portefeuille mobile.....	20
Figure 5 : Diagramme de cas d'utilisation.....	23
Figure 6 :Diagramme de séquence	24
Figure 7 :Diagramme de classe	25
Figure 8 :Android studio	30
Figure 9 :With vs without Firebase	30
Figure 10 : FIREBASE	30
Figure 11 : Base de données Realtime.....	31
Figure 12 : page d'accueil.....	31
Figure 13 : page d'inscription.....	31
Figure 14 restriction du mot de passe	32
Figure 15 Confirmation d'sms.....	32
Figure 16 envoie d'sms de confirmation.....	32
Figure 17 Page principale.....	33
Figure 18 Générer le QR CODE.....	34
Figure 19 Scanner le QR CODE.....	34
Figure 20 Message de confirmation	34
Figure 21 Message de confirmation	34
Figure 22 Mis à jour de la base de données après la transaction.....	35
Figure 23 Solde mis à jour pour Hassan.....	35
Figure 24 Solde mis à jour pour Zakaria.....	35
Figure 25 hash des identifiant des transactions	36
Figure 26 Accès aux transactions de HASSAN.....	36
Figure 27 : Accès aux transactions de ZAKARIA.....	36
Figure 28 : Accès et manipulation des comptes par l'administrateur	37

Table des matières

Remerciements.....	3
Résumé	4
Abstract.....	5
Table des figures	6
Table des matières	7
Introduction générale.....	8
I. Chapitre 1	10
1.1. Présentation du projet	10
1.2. Statistiques :	11
1.3. Problématique :	13
1.4. Objectifs :.....	13
1.5. Méthodologie de gestion de projet :	13
1.6. Planification du projet :	17
II. Chapitre 2	19
2.1 Analyse et conception.....	19
2.2 Étude et analyse des besoins.....	20
2.3 Conception :.....	23
2.4 Sécurité :	26
III. Chapitre 3	29
3.2 Outils de développement :.....	30
3.3 Réalisation :	31
Conclusion générale.....	39
Webographie.....	40

Introduction générale

Aujourd'hui, les transactions se concentrent sur l'application de la technologie de paiement mobile à des secteurs tels que la banque, la vente au détail, la restauration, les transferts d'argent, les applications, les jeux en ligne et les points de vente mobiles. Ceci aide les organisations à réaliser des économies de coûts et les avantages opérationnels.

Les cybercriminels d'aujourd'hui ne cherchent pas uniquement des informations de carte de crédit. Ils ciblent les noms d'utilisateur, les mots de passe, les adresses e-mail, les numéros de sécurité sociale, les informations de compte bancaire et d'autres données sensibles qui peuvent leur permettre de reprendre le compte d'application mobile d'un consommateur. Les reprises de compte, qui peuvent être à la base de virements de fonds ponctuels ou d'une exploitation continue, sont l'une des formes de fraude les plus répandues dans l'environnement mobile d'aujourd'hui. En réponse à ceci, notre travail consiste sur le développement et à la sécurisation d'une application mobile de paiement ou plus précisément un portefeuille électronique.

Le présent rapport est dédié à la présentation de l'ensemble des travaux menés dans le cadre du projet de fin d'année. Le premier chapitre est consacré à la description du contexte général de ce projet, en passant par la description de la problématique, ensuite l'analyse des fonctionnalités à implémenter.

Le deuxième chapitre est dédié à l'étude technique et à la conception de l'application, en étudiant en premier lieu les outils nécessaires pour la réalisation et la bonne conduite du projet, ainsi que la sécurisation de l'application et du système de paiement. Puis, en proposant en deuxième

lieu une conception technique de l'application, puis les différents diagrammes d'analyses.

Le dernier chapitre est destiné à décrire la mise en œuvre du projet, il comprend les outils choisis pour le développement ainsi que les détails des différentes phases de la réalisation de l'application.

Et enfin, la conclusion générale résume le bilan du travail effectué et principales perspectives.

Chapitre 1

I. Chapitre 1

1.1. Présentation du projet

Dans ce chapitre nous allons définir le contexte général du projet, voir les problématiques, des statistiques sur le sujet, et définir les objectifs et le processus de développement adopté pour la mise en œuvre.

Chapitre 1

1.2. Statistiques :

Les paiements numériques poursuivent leurs expansions pour devenir de plus en plus dominants en ce qui concerne les transactions financières, tandis que l'utilisation de l'argent liquide et des chèques diminue au fil des années. (1)

Bien que l'expansion du paiement numérique était lié à plusieurs facteurs, aujourd'hui, la crise économique liée à l'épidémie du coronavirus représente un tournant pour l'industrie des paiements et qui aura un impact dans les années qui suivent sur cette industrie, donc l'utilisation de ce genre de paiement est devenu indispensable surtout qu'on vient de réaliser que les opérations bancaires peuvent prendre du temps, que les frais bancaires peuvent être coûteux, et que les paiements et les transferts peuvent être lents etc. (2)

Chapitre 1

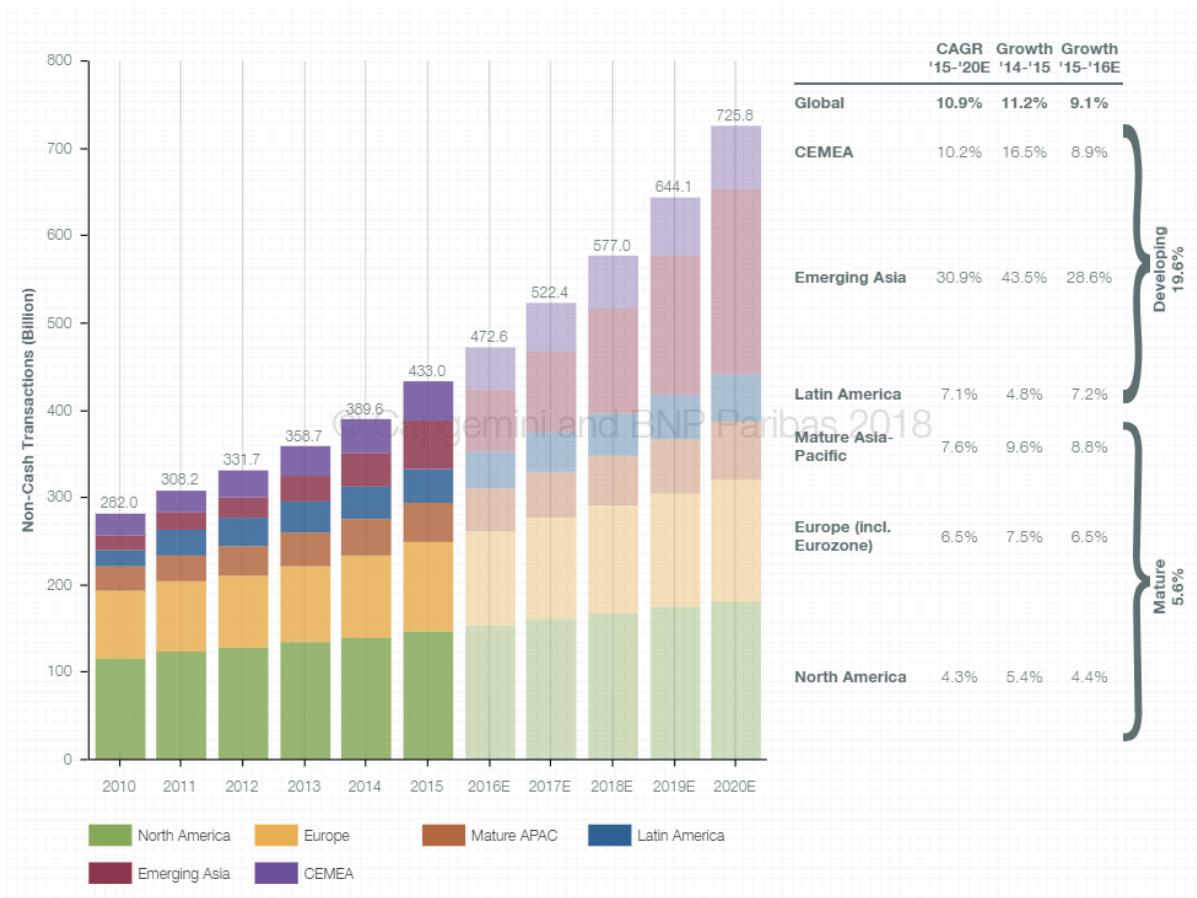


Figure 1 number of non-cash transactions worldwide for north America, Europe, mature APAC, Latin America, emerging Asia and CEMEA

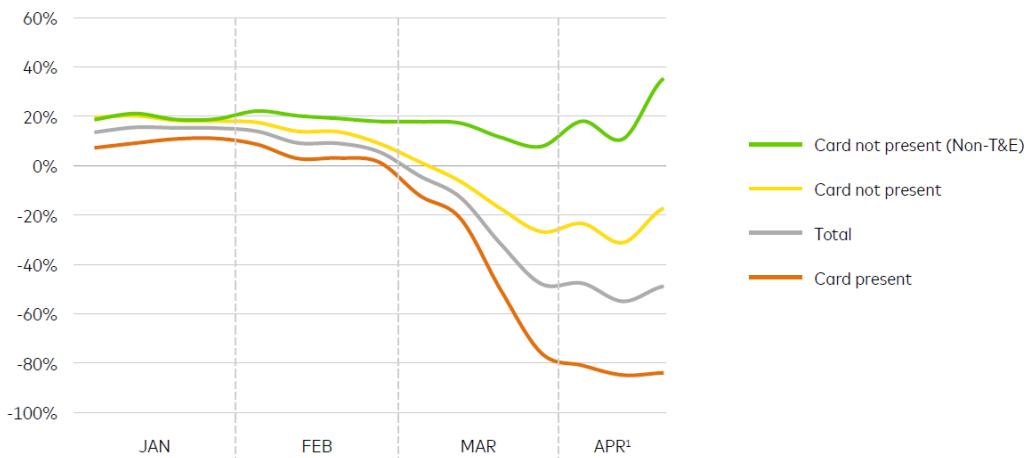


Figure 2 Cross-border volume trends

1.3. Problématique :

L'argent liquide semble moins important lorsque on peut stocker notre argent, voir notre balance payer facilement ou recevoir de l'argent avec un portefeuille électronique. Mais, l'apparition de toute nouvelle technologie est accompagnée par des risques supplémentaires, donc, la sécurisation de telles moyen de paiement est primordiale, et l'utilisation de ces technologies doit être vigilante et responsable. Donc, toute la difficulté réside sur le fait de rendre un tel moyen de manipulation d'argent une solution sûr et fiable.

1.4. Objectifs :

L'objectif de ce projet est de réaliser une application mobile E-Wallet. Cette application nous permettra de simuler le paiement mobile ; Les utilisateurs peuvent consulter leurs balances faire des échanges d'argent entre eux et consulter le journal de leurs transactions. Et bien sûr, tous ces fonctionnalités doivent être sécurisés selon des normes précises.

1.5. Méthodologie de gestion de projet :

Cette partie est destinée pour la présentation de la méthode suivie pour la gestion et la planification du projet.

Choix de la méthodologie

Le choix entre une méthode et une autre, dépend de la nature du projet et de sa taille. Pour des projets de petite taille et dont le domaine est maîtrisé, par exemple, un cycle de vie en cascade s'avère largement suffisant. Lorsqu'il s'agit d'un projet où les données ne sont pas réunies

Chapitre 1

dès le départ, où les besoins sont incomplets voire floues, il faut s'orienter vers une méthode itérative ou orientées prototypes.

Parmi les méthodes itératives, nous pouvons distinguer les méthodes AGILE largement utilisées de nos jours à travers le monde. Une méthode AGILE est menée dans un esprit collaboratif et s'adapte aux approches incrémentales.

Une méthode AGILE assure une meilleure communication avec le client en tenant compte de l'évolution de ces besoins, et une meilleure visibilité du produit livrable. Elle permet aussi de gérer la qualité en continu et de détecter des problèmes le plus tôt au fur et à mesure, permettant ainsi d'entreprendre des actions correctrices sans trop de pénalités dans les coûts et les délais.

Il y a plusieurs méthodes AGILE et il ne s'agit pas de choisir la meilleure méthode parmi celles existantes. Il s'agit plutôt de sélectionner la méthode la plus adaptée à notre projet.

La nature de projet qui doit être évolutif et dont tous les besoins n'ont pas encore été totalement identifiés, nous a orientées vers une méthode de type AGILE et plus particulièrement SCRUM.

Présentation de la méthodologie SCRUM

Le principe de la méthodologie SCRUM est de développer un logiciel de manière incrémentale en maintenant une liste totalement

Chapitre 1

transparente des demandes d'évolutions ou de corrections à implémenter. Avec des livraisons très fréquentes, toutes les 4 semaines en moyenne, le client reçoit un logiciel fonctionnel à chaque itération. Plus nous avançons dans le projet, plus le logiciel est complet et possède toujours de plus en plus de fonctionnalités. Pour cela, la méthode s'appuie sur des développements itératifs à un rythme constant d'une durée de 1 à 4 semaines.

Les sprints durent généralement deux à quatre semaines. Durant un sprint, il y a toujours des réunions quotidiennes entre les différents collaborateurs du projet afin de présenter l'état d'avancement des différentes tâches en cours, les difficultés rencontrées ainsi que les tâches restantes à réaliser.

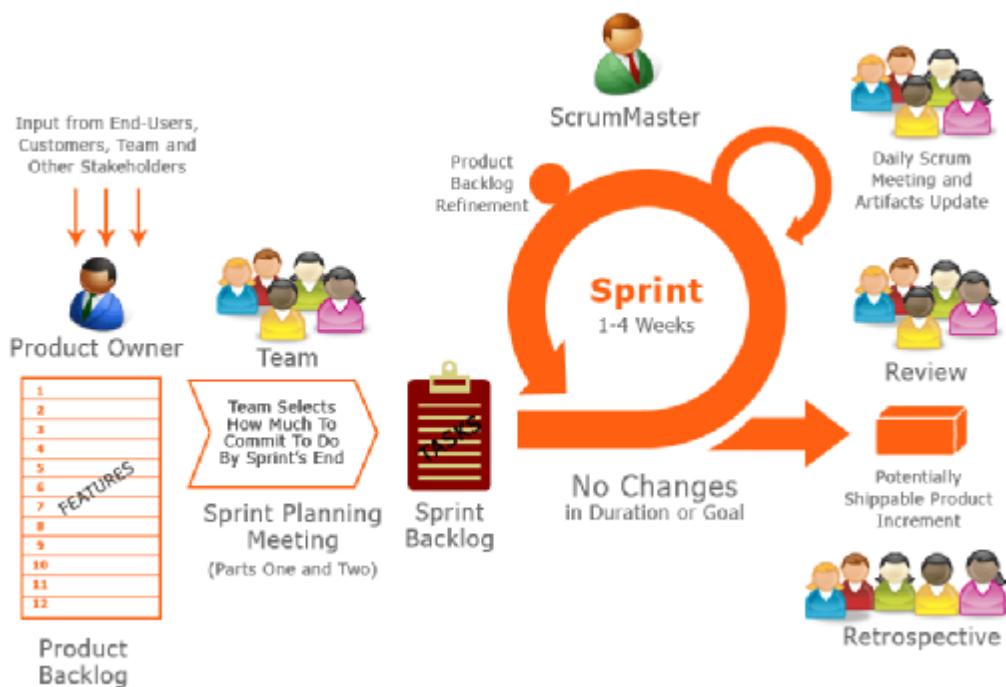


Figure 3 Schéma du processus de la méthode agile SCRUM

Chapitre 1

Principes essentiels de la méthode :

- L'équipe : nous nous concentrons sur les personnes et leurs interactions plutôt que sur les processus et les outils.
- L'application : le plus important c'est d'avoir une application fonctionnelle plutôt que d'avoir une documentation complète.
- La collaboration : cette méthode se base sur la collaboration avec le client.
- L'acceptation du changement : nous ne suivons pas un plan fixe mais nous réagissons à chaque nouveau changement.

Organisation :

La méthodologie SCRUM fait intervenir 3 rôles principaux qui sont :

- ❖ **Product Owner** : dans la majorité des projets, le responsable produit (Product Owner) est le responsable de l'équipe projet client. C'est lui qui va définir et prioriser la liste des fonctionnalités du produit et choisir la date et le contenu de chaque sprint sur la base des valeurs (charges) qui lui sont communiquées par l'équipe.
- ❖ **Scrum Master** : véritable facilitateur sur le projet, il veille à ce que chacun puisse travailler au maximum de ses capacités en éliminant les obstacles et en protégeant l'équipe des perturbations extérieures. Il porte également une attention particulière au respect des différentes phases de SCRUM.
- ❖ **Equipe** : l'équipe s'organise elle-même et elle reste inchangée pendant toute la durée d'un sprint. Elle doit tout faire pour délivrer le produit.

Chapitre 1

1.6. Planification du projet :

Avant de démarrer, il était essentiel de prévoir une planification de la réalisation et la mise en œuvre de chaque sprint du projet. L'objectif du planning consiste à déterminer et à ordonner les tâches, à estimer leurs charges et à déterminer les pré requis nécessaires à leur réalisation et valider séquentiellement en vue d'assurer sa conformité avec les besoins exprimés.

Les étapes de la planification étaient élémentaires ; chaque étape consiste sur une classification des tâches, la formation sur les outils du développement, la réalisation et le test des outils utilisés loin de notre projet, puis l'implémentation et le de ces outils pour pouvoir revenir à la version précédente en cas d'échec et le test et la validation.

Chapitre 1

1.7. Conclusion :

Dans ce chapitre, nous avons décrit le cadre du projet, les objectifs généraux à atteindre, puis nous avons donné une idée globale sur la méthodologie de conduite du projet à l'aide de SCRUM.

Chapitre 2

II. Chapitre 2

2.1 Analyse et conception

Ce chapitre abordera le cahier de charge, l'aspect de sécurité, ainsi que l'approche et la modélisation de l'application.

2.2 Étude et analyse des besoins

Étude de besoin :

L'E-Wallet offre une solution de paiement sécurisée et fiable et garantit que la transaction se déroule rapidement. Les portefeuilles mobiles permettent d'envoyer des espèces depuis un smartphone, soit à une autre personne, soit à un terminal de paiement en un clic, ce qui rend la transaction simple et rapide.

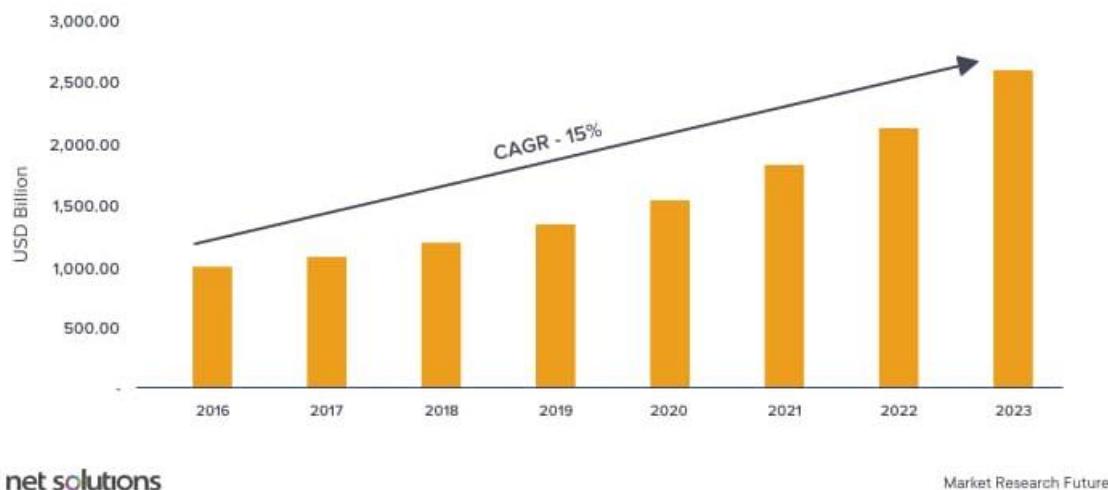


Figure 4 Croissance globale de projet de portefeuille mobile

Les dernières années ont vu une forte augmentation des systèmes de paiement numérique. Grâce à la transformation numérique, l'application de portefeuille mobile semble dominer le marché des paiements en ligne et est de plus en plus préférée pour des transactions rapides et sans tracas. De plus, c'est un moyen facile pour se débarrasser du temps d'attente pour payer des factures ou transférer de l'argent.

Chapitre 2

Cahier de charge :



- Confidentialité et sécurité :

Un portefeuille électronique attend des utilisateurs qu'ils stockent leurs informations de leurs cartes et saisissent leurs mots de passe. Ainsi, l'application doit être capable de sécuriser les données des utilisateurs. Étant donné que les applications de portefeuille sont toujours une cible souple pour les pirates, l'application doit être protégée par un mot de passe avec des fonctionnalités telles que l'empreinte digitale et le QR code pour une authentification et une validation appropriée, en plus d'un transfert de paiement sécurisé, rapide et efficace.



- Facilité d'utilisation et transaction transparente :

Le traitement d'un paiement via un portefeuille mobile est rapide et fluide. L'application enregistre les informations pour l'authentification et offre une transaction sécurisée et transparente.



- Technologie basée sur le cloud :

Avec cette fonctionnalité, les transactions sont faites de manière sécurisée. La technologie basée sur le cloud offre aux clients la suite complète de capacités pour transformer leurs smartphones en portefeuilles numériques.

Chapitre 2



- Paiement par QR CODE :

L'utilisateur voulant recevoir l'argent génère un QR CODE après avoir saisi la somme, puis l'utilisateur voulant payer scan ce QR CODE pour finaliser la transaction.



- Inscription d'un nouvel utilisateur :

Un SMS de confirmation est envoyé à l'utilisateur voulant s'inscrire pour confirmer et finaliser l'inscription.



- Accès aux Transactions :

L'utilisateur peut accéder à tout moment à la liste de ses transactions et peut en chercher une à l'aide d'une barre de recherche.

2.3 Conception :

Les cas d'utilisation :

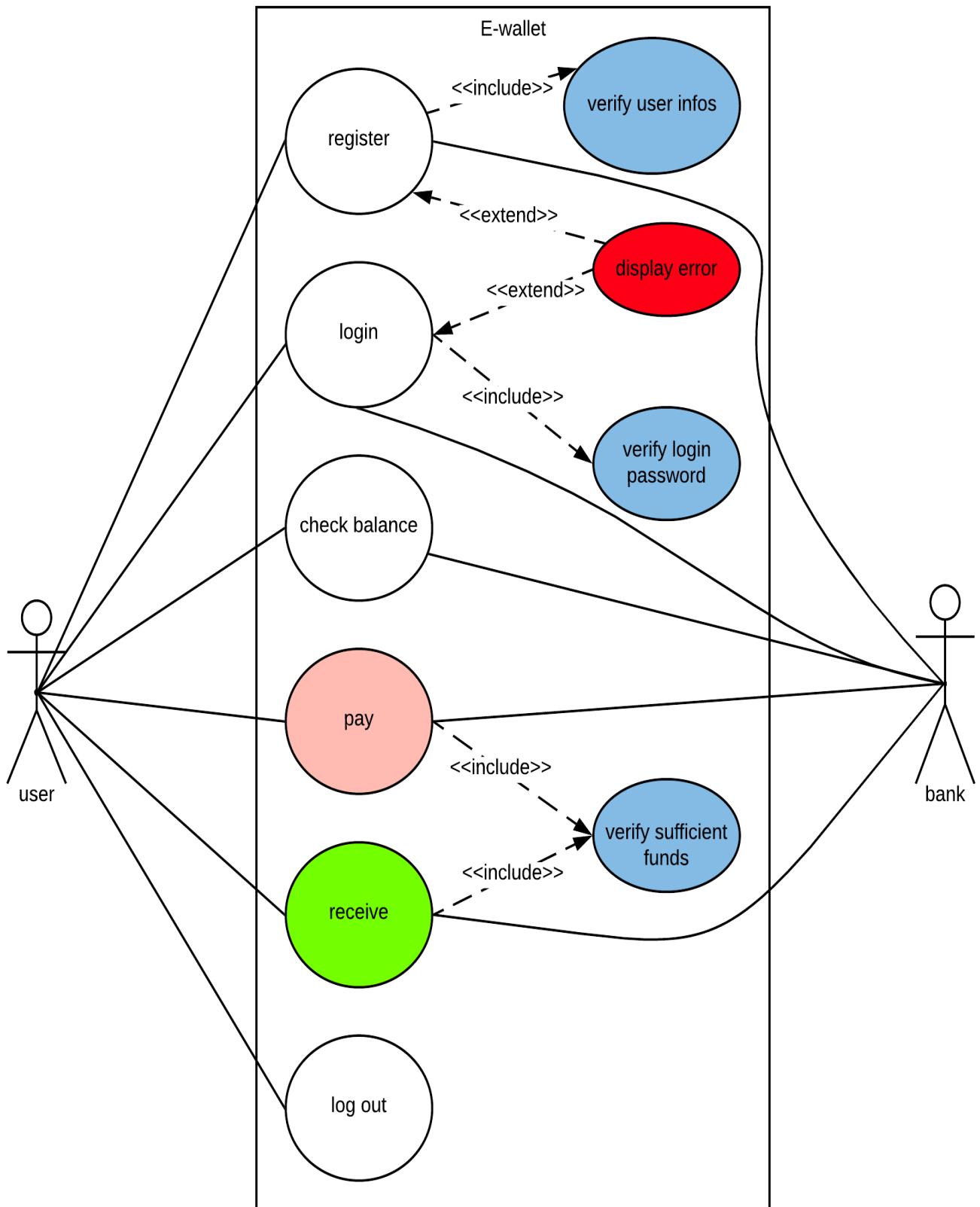


Figure 5 Diagramme de cas d'utilisation

Chapitre 2

Diagramme de séquence :

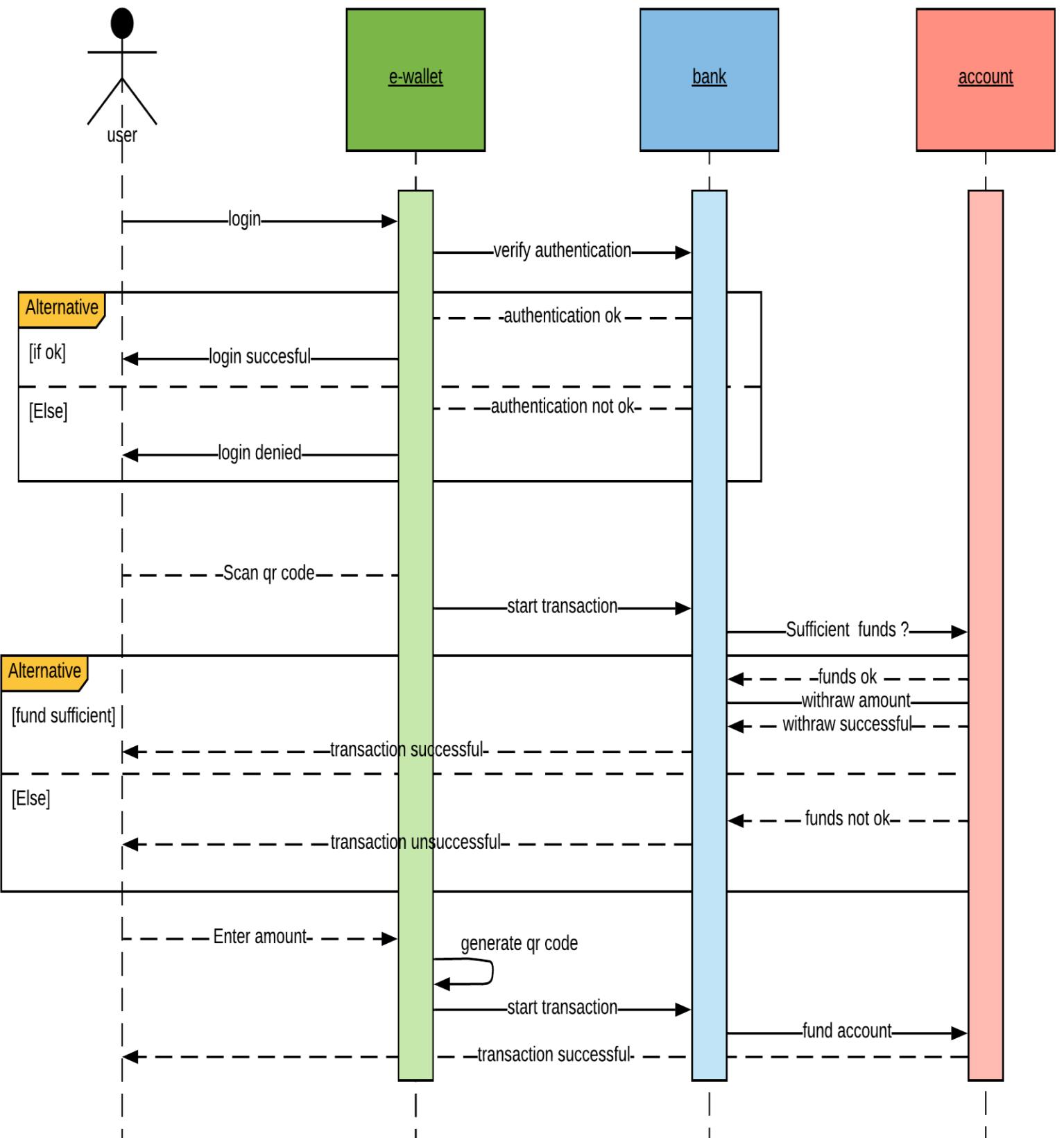


Figure 6 Diagramme de séquence

Chapitre 2

Diagramme de classe :

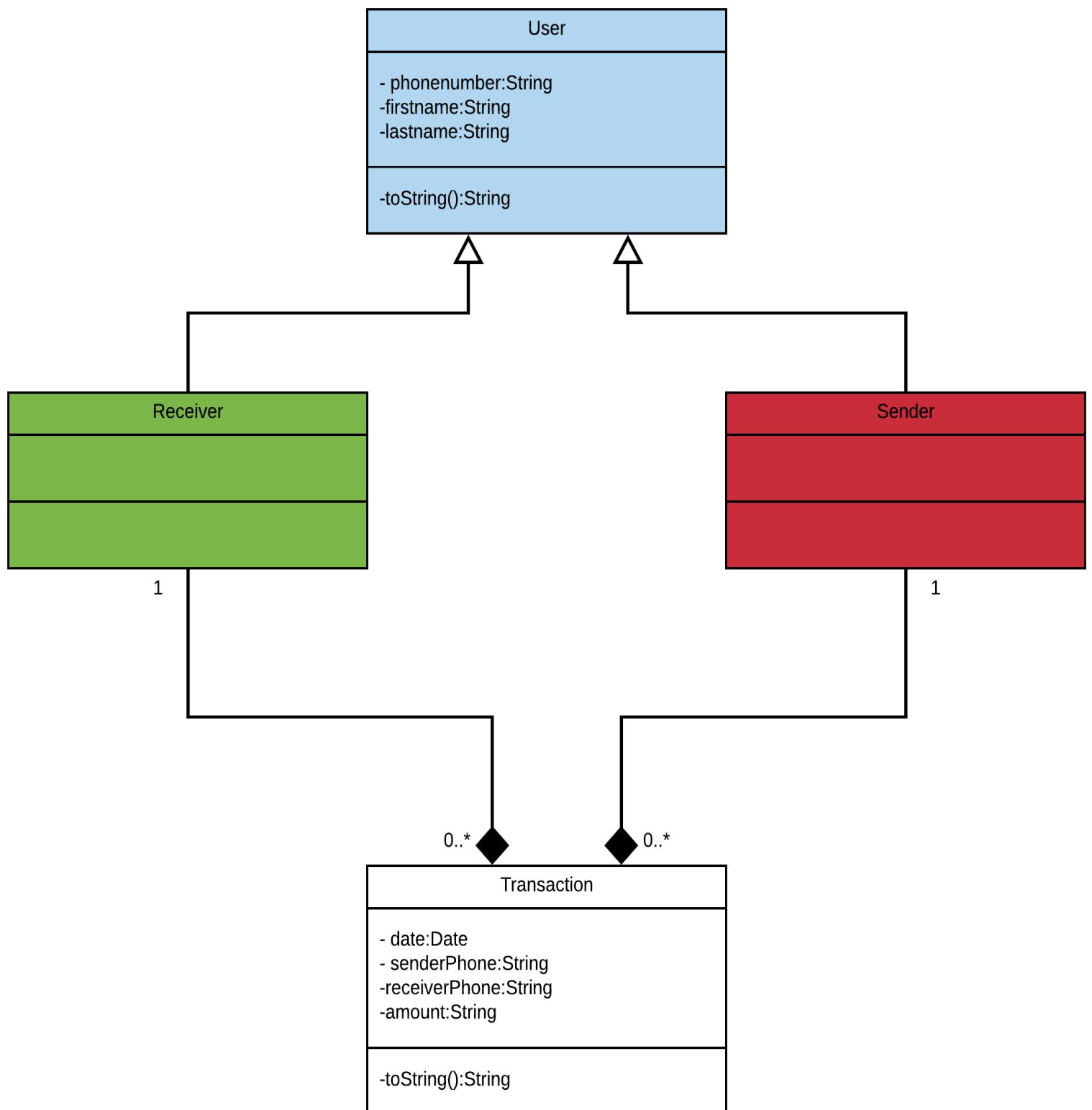


Figure 7 Diagramme de classe

2.4 Sécurité :

Les smartphones sont vulnérables aux mêmes risques que les ordinateurs personnels, mais ils offrent également des fonctionnalités de communication supplémentaires qui peuvent augmenter le potentiel de risques de sécurité. (3)



Pour minimiser ces risques, les données sensibles ne doivent jamais être stockées sur des appareils mobiles, y compris les données de suivi des numéros de cartes de paiement ou l'API identifiant de connexion ou clé de transaction pour les paiements mobiles. (3)



Pour plus de sécurité un nouvel appareil mobile doit être enregistré et approuvé avant de pouvoir être utilisé si vous testez votre demande, l'étape d'enregistrement et d'approbation est obligatoirement effectuée.

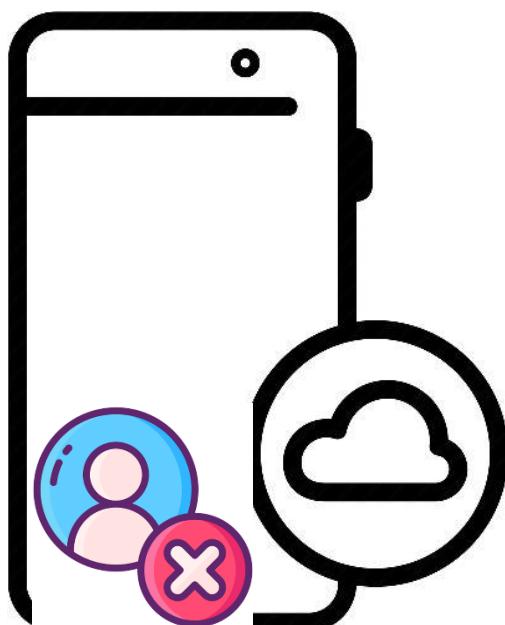


Chapitre 2

Une fois enregistré et approuvé les utilisateurs peuvent simplement se connecter à l'application mobile avec leurs ID de connexion et mot de passe de l'interface du marchand et accepter les paiements mobiles. (3)



Discutons maintenant les éléments requis pour soumettre une transaction. Les transactions soumises depuis les appareils mobiles doivent inclure le bloc d'authentification de l'utilisateur qui inclut l'identifiant de connexion le token de session valide et ID d'appareil mobile unique le dernier élément requis est le bloc de demande de transaction qui doit inclure au moins le montant du paiement la date et l'identifiant de l'expéditeur et du destinataire. (3)



L'application ne doit jamais stocker ces informations d'identification sur le mobile appareil lui-même les appareils mobiles peuvent être désactivé s'ils ne sont plus utilisés ou sont Perdu ou volé. (3)

Chapitre 2

2.5 Conclusion :

Nous avons vu dans ce chapitre l'analyse qui va servir pour mieux comprendre le système et les besoins. Elle a fourni des lignes directrices pour construire la solution, une conception technique sur laquelle on va se baser pour créer l'application.

Quant au chapitre suivant, il est consacré à l'étude technique et la réalisation de notre solution.

Chapitre 3

III. Chapitre 3

3.1 Réalisation et mise en œuvre :

Ce chapitre aborde la mise en œuvre et la réalisation, en présentant les outils de réalisation ainsi que le travail réalisé.

3.2 Outils de développement :

Langages de programmation et développement

Android studio :

Android Studio est l'environnement de développement intégré (IDE) officiel du système d'exploitation Android de Google, construit sur le logiciel IntelliJ IDEA de JetBrains et conçu spécifiquement pour le développement Android. Android Studio offre la solution la plus rapide pour développer des applications performantes et de qualité destinée aux appareils Android, y compris les téléphones et les tablettes, Android Auto, Android Wear et Android TV. En tant qu'environnement de développement intégré officiel de Google, Android Studio inclut tout ce dont un développeur a besoin.

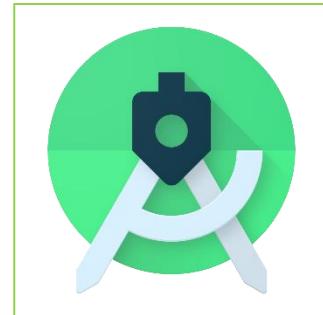


Figure 8 Android studio

Firebase :

Firebase est une plateforme de développement d'applications mobiles et Web. Différemment du développement d'applications traditionnel, qui implique généralement l'écriture du backend et du frontend, Le frontend code appelle simplement les points de terminaison API exposés par le backend, et le backend fait le travail. Cependant, avec les produits Firebase, le backend traditionnel est contourné. L'accès administratif à chacun de ces produits est fourni par la console Firebase par le développeur. (4)



Figure 10 FIREBASE

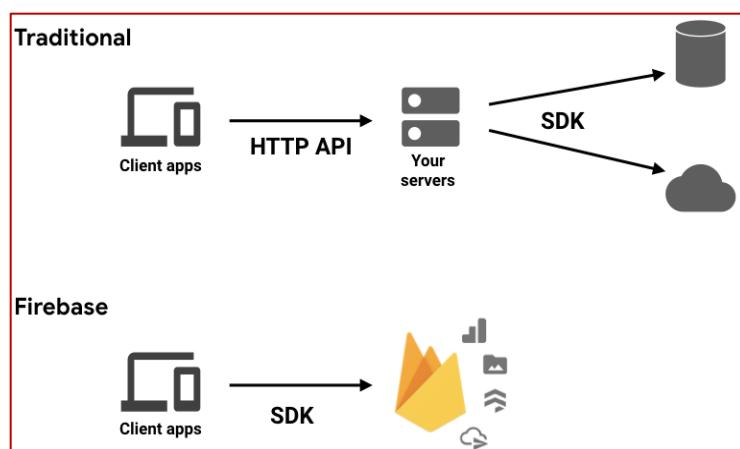


Figure 9 With vs without Firebase

Chapitre 3

The screenshot shows the Firebase Realtime Database interface. On the left, there's a sidebar with 'Développer' (Authentication, Database, Storage, Hosting, Functions, ML Kit), 'Qualité' (Crashlytics, Performance, Test Lab...), and 'Extensions'. The main area is titled 'Database' with tabs for 'Données', 'Règles', 'Sauvegardes', and 'Utilisation'. A sub-section 'wallet 1.0' is selected. The database structure is displayed as a tree: 'User' contains 'Phone Number' (with values 0609657728, 0619865034, 0669405677) and 'les Transactions' (with values 2caa31d1a6fd294fc1a00947d510cde4f0d8be1d6345d9a58c32213d1f2cecb4, 4576832eb166557ddcd9aa29f288142d1cf492d8c62c665177ef39a9e14a8ac8, 7687cb1156b7665b92db42dd79f44a40172772b1b03844c9724253c1b93b511, 81b135f685360d1b5f770617be1714e9e52ea797bcceada609ef30bef7d06bd5). At the top right, there are links to 'Accéder à la documentation' and a help icon.

Figure 11 Base de données Realtime

3.3 Réalisation :

L'objectif de cette partie est de donner aux lecteurs de ce rapport un petit aperçu sur les fonctionnalités de l'application ou nous allons voir un scenario d'utilisation qui englobera toutes les fonctionnalités de l'application.

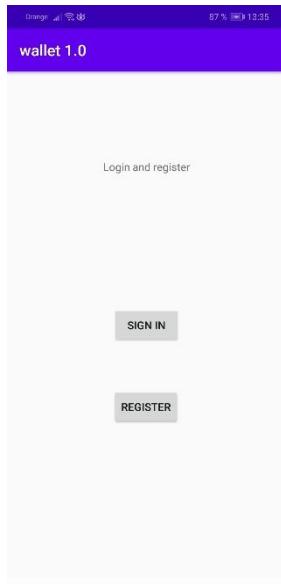


Figure 12 page d'accueil

La page d'accueil permet à l'utilisateur, grâce aux boutons 'SIGN IN' et 'REGISTER', de se connecter si l'utilisateur possède déjà un compte ou de s'inscrire dans le cas d'une première utilisation.

This is a screenshot of the registration screen of the mobile application. The top bar shows signal strength, battery level at 88%, and the time 13:35. The title 'wallet 1.0' is at the top. There is a 'SIGN IN' button in the top right corner. The form is titled 'Registration' and includes fields for 'FIRST NAME*', 'LAST NAME', 'PASSWORD*', 'CONFIRM PASSWORD*', and 'PHONE*'. At the bottom, there are three navigation icons: a triangle pointing left, a circle, and a square, followed by a 'FORWARD' button.

Figure 13 page d'inscription

Chapitre 3

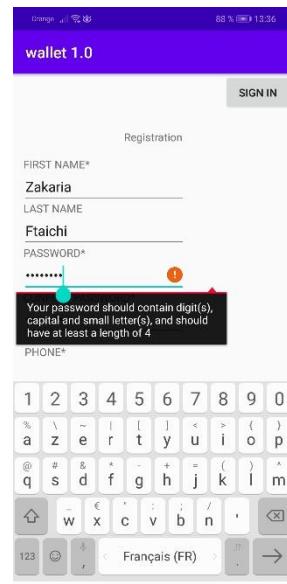


Figure 14 restriction du mot de passe

```
/* regular express */
onlyChars = Pattern.compile("^[A-Z]*[a-z]*$");
passwordCheck = Pattern.compile("^(?=.*[a-z])(?=.*[A-Z])(?=.*\d)[A-Za-z\d]{4,20}$");
```

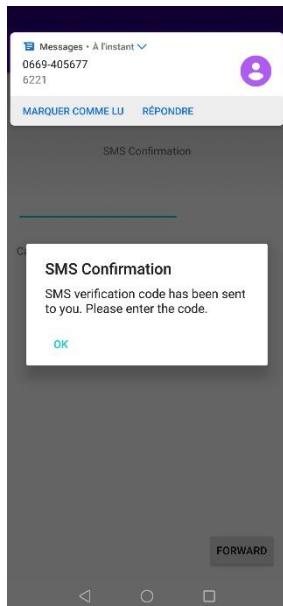


Figure 16 envoie d'sms de confirmation

Dans le cadre de la sécurisation de l'application un sms de confirmation est envoyé à l'utilisateur voulant s'inscrire pour s'assurer que le numéro de téléphone saisi est celui de l'utilisateur même.

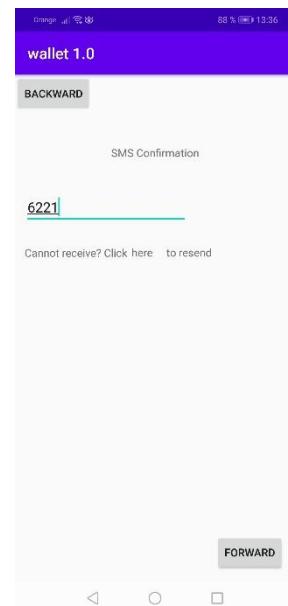
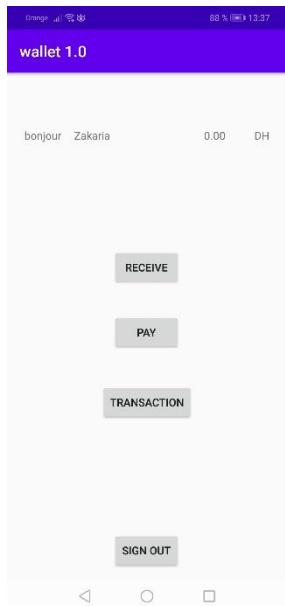


Figure 15 Confirmation d'sms

Chapitre 3



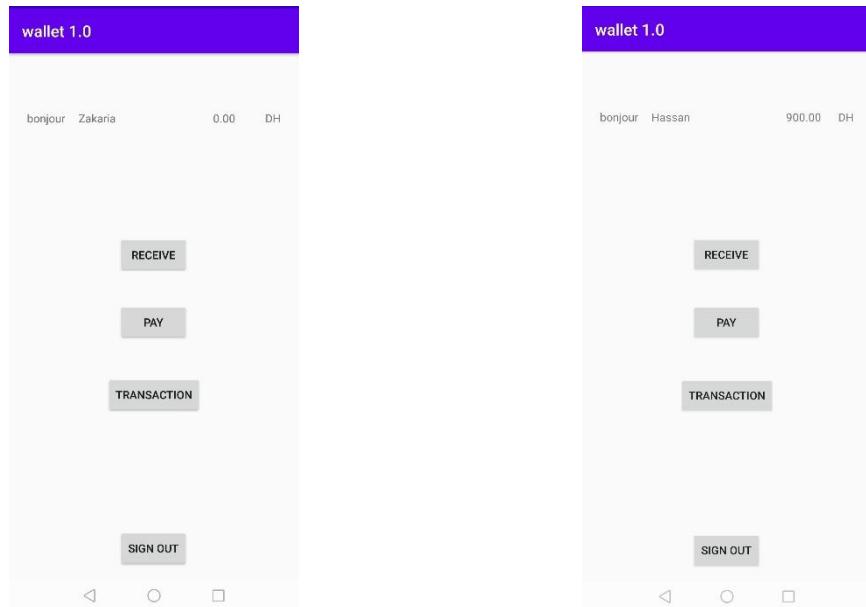
L'utilisateur est maintenant connecté, il peut voir son solde, et grâce aux trois boutons ‘**RECEIVE**’, ‘**PAY**’ et ‘**TRANSACTION**’, il peut recevoir de l'argent, payer, ou voir ses transactions.

Tous ces informations sont stockées dans la base de données real time ce qui fait qu'elles sont synchronisées en temps réel.

Figure 17 Page principale

Payer et recevoir :

La partie qui suit illustre une transaction entre deux utilisateurs, ‘Hassan’ et ‘Zakaria’.



Chapitre 3

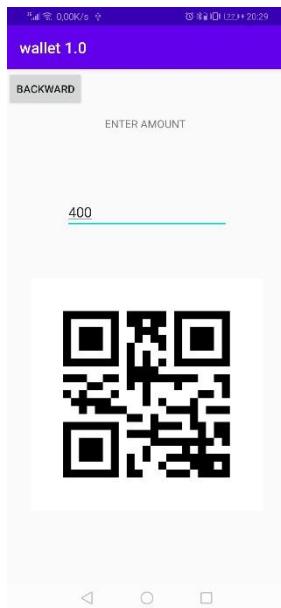


Figure 18 Générer le QR CODE

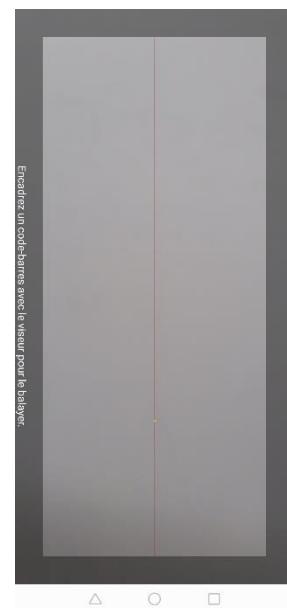


Figure 19 Scanner le QR CODE

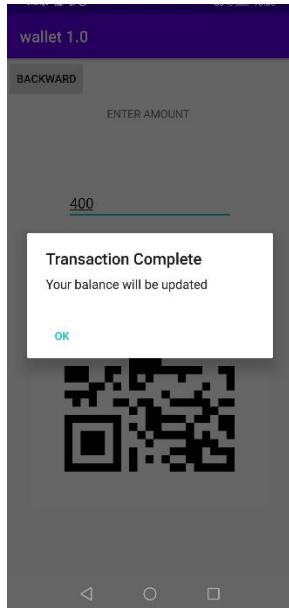


Figure 20 Message de confirmation

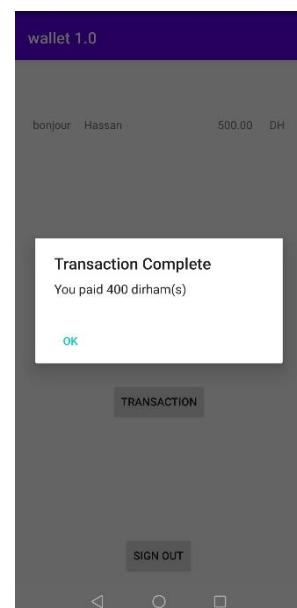


Figure 21 Message de confirmation

Chapitre 3

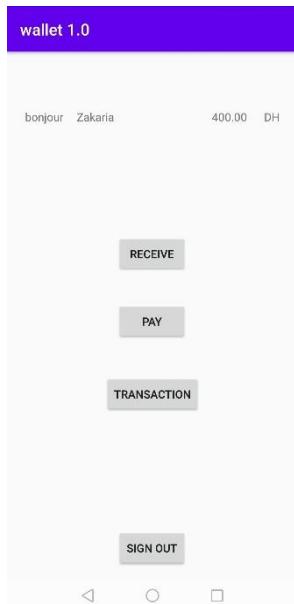


Figure 24 Solde mis à jour pour Zakaria

Après le scanne du code, le solde est mis à jour, et la transaction est enregistrée dans la base de données. Les utilisateurs peuvent voir leurs soldes sur la page ‘home’ et peuvent consulter leurs transactions avec le bouton ‘Transaction’. Dans l’autre côté l’administrateur peut accéder à ces informations grâce à la console de Firebase.

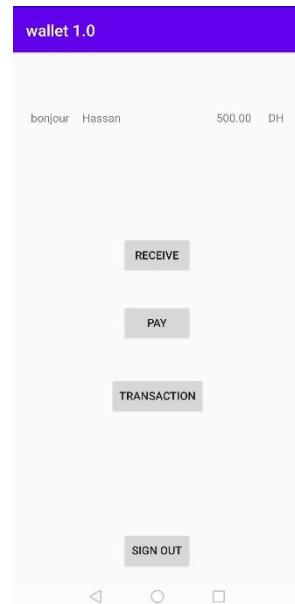


Figure 23 Solde mis à jour pour Hassan

The screenshot shows the Firebase Realtime Database interface with the URL <https://wallet-1-0.firebaseio.com/>. The database structure is as follows:

- wallet-1-0**:
 - User**:
 - Phone Number**:
 - 0609657728**:
 - balanceAmount: "50000"**
 - firstName: "Hassan"**
 - lastName: "Eloufir"**
 - mes Transactions**:
 - 7687cb1156b7665b92dbb42dd79f44a40172772b1b03844c9724253c1b93b511**:
 - amount: "- 400 dh"**
 - date: "2020/06/01 13:38:31"**
 - receiverPhone: "0669405677"**
 - 81b135f685360d1b5f770617be1714e9e52ea797bcceada609ef30bef7d06bd5**
 - 0619865034**
 - 0669405677**:
 - balanceAmount: "40000"**
 - firstName: "Zakaria"**
 - lastName: "Ftaichi"**
 - mes Transactions**:
 - 7687cb1156b7665b92dbb42dd79f44a40172772b1b03844c9724253c1b93b511**:
 - amount: "+ 400 dh"**
 - date: "2020/06/01 13:38:31"**
 - senderPhone: "0609657728"**
 - les Transactions**:
 - 2caa31d1a6fd294fc1a00947d510cde4f0d8be1d6345d9a58c32213d1f2cecb4**
 - 4576832eb166557ddcd9aa29f288142d1cf492d8c62c665177ef39a9e14a8ac8**
 - 7687cb1156b7665b92dbb42dd79f44a40172772b1b03844c9724253c1b93b511**
 - 81b135f685360d1b5f770617be1714e9e52ea797bcceada609ef30bef7d06bd5**

Figure 22 Mis à jour de la base de données après la transaction

Chapitre 3

Avant d'être enregistrées, un hash est calculé et attribué à la transaction. (Le hash est celui de la chaîne de caractère constituée des informations de la transaction comme la date le montant le numéro de l'envoyeur et du receveur).

```
DateTimeFormatter dtf = DateTimeFormatter.ofPattern("yyyy/MM/dd HH:mm:ss");
LocalDateTime now = LocalDateTime.now();
String date = dtf.format(now);
String TransactionId = sender+receiver+transactionAmount+date;
TransactionToFirebase PayT = new TransactionToFirebase(receiver, Amount: "- " + transactionAmount + " dh", date, r: 0);
TransactionToFirebase ReceiverT = new TransactionToFirebase(sender, Amount: "+" + transactionAmount + " dh", date);
TransactionToFirebase T = new TransactionToFirebase(sender, receiver, Amount: transactionAmount + " dh", date);
```

Figure 25 hash des identifiant des transactions

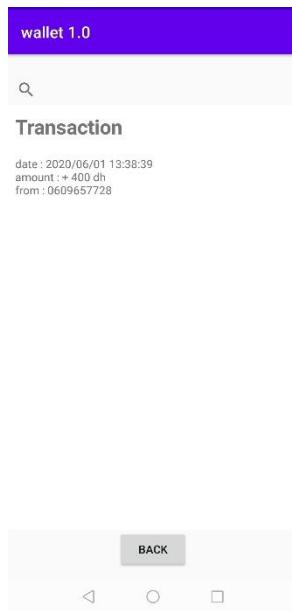


Figure 27 Accès aux transactions de ZAKARIA

Cette étape concerne la consultation des transactions. Grâce au bouton ‘Transaction’, les utilisateurs accède à leurs transactions et peuvent chercher une transaction à l'aide de la barre de recherche se trouvant en haut de l'écran.



Figure 26 Accès aux transactions de HASSAN

Chapitre 3

Enfin, grâce à la plateforme Firebase l'administrateur peut gérer les comptes des utilisateurs, il réinitialiser le mot de passe, désactiver ou supprimer un compte.

The screenshot shows the Firebase Authentication interface under the 'Users' tab. It displays a list of three users with their email addresses, provider icons, creation dates, last sign-in dates, and unique IDs. A context menu is open over the first user's row, listing options: 'Réinitialiser le mot de passe' (Reset password), 'Désactiver le compte' (Disable account), and 'Supprimer le compte' (Delete account). The interface includes a search bar, a blue 'Ajouter un utilisateur' (Add user) button, and pagination controls at the bottom.

Identifiant	Fournisseurs	Date de création	Dernière connexion	ID utilisateur ↑
0609657728@mail.com	✉	25 avr. 2020	1 juin 2020	a953D00dq1
0669405677@mail.com	✉	1 juin 2020	1 juin 2020	cJ8JgEsu3aN
0619865034@mail.com	✉	25 avr. 2020	25 avr. 2020	cgSiVqIT7aZsQQLr83rZH3MzFmtl

Figure 28 Accès et manipulation des comptes par l'administrateur

Chapitre 3

3.4 Conclusion :

Nous avons vu dans ce chapitre qui était consacré à l'étude technique et la réalisation de notre solution, les différents outils utilisés comme langages de programmations, environnement de développement et bases de données ainsi que la majorité des cas d'utilisations de l'application.

Conclusion générale

Appart les fonctionnalités principales d'un portefeuille électronique comme la possibilité de stocker son argent, consulter son solde, faire des transactions, il était nécessaire de se concentrer aussi sur la sécurité de ce système de paiement. Pour ceci nous avons essayé de respecter aux maximum les normes de développement d'une application de paiement mobile, comme la confidentialité, les sms de confirmations, la gestion des données, surtout que l'application interagit avec des données de grande valeur. Par faute de temps, nous avons mis sur notre cahier de charge des tâches que nous n'avons pas pu réaliser, et qui font partie des normes de sécurités, comme l'implémentation des jetons qui représentent un excellent outil pour contrôler, et sécuriser l'accès aux comptes ainsi que l'effectuation des transactions. Pourtant, la sécurité n'est jamais absolue, et doit se développer constamment pour s'adapter avec les nouvelles technologies.

Webographie

1. MANCHANDA, AMIT.

<https://www.netsolutions.com/insights/essential-features-for-building-popular-mobile-wallet-app/>. Consulté le 12 février 2020.

2. Rooney, Kate. <https://www.cnbc.com/2020/04/29/mastercard-sees-40percent-jump-in-contactless-payments-due-to-coronavirus.html>. Consulté le 29 avril 2020.

3. Developers, PCI Mobile Payment Acceptance Security Guidelines for. https://www.pcisecuritystandards.org/documents/PCI_Mobile_Payment_Acceptance_Security_Guidelines_for_Developers_v2_0.pdf. Consulté le 29 02 2020.

4. Stevenson, Doug. <https://medium.com/firebase-developers/what-is-firebase-the-complete-story-abridged-bcc730c5f2c0>. Consulté le 05 mars 2020.