**DEFINITIONS**

**Système**: ensemble d’éléments qui interagissent ensemble entre eux et aussi avec l’environnement pour un but

**Système d’information** : ensembles de ressources qui permettent de capter, traiter, stocker et diffuser de l’information

**Système d’information de wave** : système d’information qui est lié à la gestion financière (faire les transactions financières : envoie retrait dépôt paiement)

**LES ETAPES DE LA CONCEPTION DU SYSTEME DE WAVE**

**1. Quel est l’objectif ?** Son objectif principal est de fournir une solution de gestion financière simple, efficace et a coût réduit

**2. Qui va l’utiliser ?** petites et grandes entreprises, particuliers, banques

**3. Que va faire chaque acteur avec le système** **?** envoie d’argent, réception d’argent, paiement électronique

4. Quelles sont les règles de gestion ?

5. Quelles sont les données ?

6. Définir l’architecture :

Les modules

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **MODULES** | **PAIEMENT** | **GESTION DES AGENTS** | **SECURITE ET GESTION DE COMPTE** | **TRANSFERT D’ARGENT** | **INTEGRATION BANCAIRE ET PORTEFEUILLE** |
| **ACTEURS** | **-Utilisateur** : Celui qui utilise son compte Wave pour payer des factures ou des commerçants.  **-Commerçant** : Les commerçants partenaires qui acceptent les paiements via Wave, souvent à travers des identifiants QR ou des interfaces dédiées.  **-Fournisseurs de services publics** : Entités comme la CIE, la SODECI , ou tout autre structure qui reçoivent des paiements pour les factures via la plateforme Wave. | **-Agent Wave** : Personne ou entreprise qui sert de point d'accès pour les dépôts et retraits d'argent, en interagissant directement avec les utilisateurs.  **-Utilisateur** : Celui qui interagit avec les agents pour déposer ou retirer de l'argent en espèces.  **-Superviseur d'agents** : Celui qui contrôle et gère l'activité des agents, notamment pour garantir la conformité aux règles de la plateforme. | **-Utilisateur** : Celui qui détient un compte Wave et gère sa sécurité, notamment par la configuration des codes PIN et l'authentification des transactions.  **-Support technique** : Équipe qui aide les utilisateurs à résoudre les problèmes de sécurité (réinitialisation de compte, verrouillage, etc.) et assurer le bon fonctionnement des systèmes de sécurité.  **-Administrateur système** : Responsable de la gestion technique du système et de la sécurité des comptes à un niveau global. | **-Utilisateur (expéditeur)** : Celui qui initie et envoie de l'argent à un autre utilisateur via l'application.  **-Utilisateur (destinataire)** : Celui qui reçoit le transfert d'argent instantanément sur son compte Wave.  **-Agent** : Intermédiaire qui peut faciliter les transferts d'argent pour les utilisateurs n'ayant pas accès direct à l'application. | **-Utilisateur** : Celui qui lie son compte bancaire à son compte Wave pour faciliter les transferts et gérer son portefeuille.  **-Banque partenaire** : Institution financière qui travaille avec Wave pour permettre les transferts entre un compte bancaire et un compte Wave.  **-Fournisseurs de services de paiement** : Acteurs externes qui gèrent les transactions bancaires et les services de paiement via carte bancaire ou d'autres plateformes de transfert. |
| **FONCTIONNALITES** | **-Paiement de factures** : Les utilisateurs peuvent régler des factures de services publics (électricité, eau, télécommunications) directement via l'application ou par USSD.  **-Paiement aux commerçants** : paiement sécurisé aux commerçants partenaires via des QR codes ou des identifiants d'utilisateur.  **-Historique des paiements** : Les utilisateurs peuvent consulter un historique détaillé de leurs paiements effectués, classés par date et type de transaction. | **-Dépôt d'espèces** : Les agents enregistrés peuvent recevoir des dépôts d'espèces de la part des utilisateurs et créditer instantanément leurs comptes.  **-Retrait d'espèces** : Les utilisateurs peuvent retirer de l'argent en espèces auprès des agents, qui débiteront leur compte.  **-Suivi des transactions** : Les agents peuvent suivre et gérer leurs transactions via une interface dédiée, avec la possibilité de vérifier l'état des dépôts et des retraits. | **-Gestion des codes PIN** : Les utilisateurs peuvent configurer et modifier leur code PIN pour sécuriser l'accès à leur compte.  **-Authentification et validation des transactions** : Chaque transaction est validée par un code PIN ou par un facteur d'authentification supplémentaire (authentification à deux facteurs).  **-Verrouillage et déverrouillage de compte** : En cas de perte de téléphone ou de soupçon de fraude, les utilisateurs peuvent verrouiller temporairement leur compte pour éviter tout accès non autorisé. | - **Envoi d'argent entre utilisateurs** : envoyer de l'argent instantanément à d'autres utilisateurs via leur numéro de téléphone.  **-Réception de transferts** : Les utilisateurs peuvent recevoir des transferts d'argent directement sur leur compte, qu'ils soient émis par un autre utilisateur ou un agent.  **-Notification en temps réel** : expéditeur et destinataire reçoivent des notifications instantanées après le transfert. | **-Liaison avec des comptes bancaires** : Les utilisateurs peuvent lier leur compte bancaire à leur compte Wave pour faciliter les transferts d'argent entre la banque et Wave.  **-Recharge de portefeuille électronique** : Les utilisateurs peuvent ajouter des fonds à leur compte à partir d'une carte bancaire ou d'un compte externe.  **-Transferts internationaux** : transferts d'argent internationaux à partir de certaines banques partenaires en fonction des accords régionaux. |
| **REGLE DE GESTION** | **-Authentification des paiements** : Chaque transaction (paiement de factures ou à des commerçants) doit être validée par un code PIN pour garantir que l'utilisateur autorise le paiement.  **-Commissions pour les paiements** : Wave peut appliquer des frais de service pour les paiements de factures ou pour les paiements aux commerçants, bien que certains services puissent être gratuits.  **-Historique des transactions**: Les utilisateurs doivent avoir accès à l’historique de leurs paiements pendant une durée minimum (par exemple 12 mois) pour vérifier les transactions passées.  **-Politique de remboursement** :  Les commerçants et fournisseurs de services publics doivent se conformer à la politique de remboursement de Wave, en cas d’erreur de transaction ou d’insatisfaction du client. | **-Formation et certification des agents** : Chaque agent doit suivre une formation obligatoire pour être autorisé à offrir des services de dépôt et retrait. Cette formation couvre les règles de gestion des transactions et la sécurité des opérations.  **-Commissions des agents** :  Les agents perçoivent une commission pour chaque transaction (dépôt ou retrait) qu'ils réalisent. Les pourcentages de commission sont définis par Wave et peuvent varier en fonction des volumes de transactions.  **-Traçabilité des transactions**: Chaque transaction effectuée par un agent doit être enregistrée avec des détails précis (nom de l’utilisateur, montant, heure, etc.) pour assurer une traçabilité complète.  **-Contrôle des liquidités** :  Les agents doivent respecter des règles strictes sur la gestion des liquidités, notamment en termes de montants minimums ou maximums de liquidités qu’ils doivent conserver pour assurer un service constant. | **-Gestion des codes PIN** :  Chaque utilisateur doit définir un code PIN sécurisé pour accéder à son compte Wave et valider les transactions. Ce code doit être changé régulièrement pour des raisons de sécurité.  **-Authentification à deux facteurs (2FA)** : Pour certaines transactions sensibles (montants élevés, modification des informations personnelles), Wave peut exiger une authentification à deux facteurs.  **-Suspension de compte** :  En cas de tentative d’accès frauduleux ou d’échec répété de saisie du code PIN, le compte de l’utilisateur peut être temporairement verrouillé.  **-Politique de récupération de compte** :  Si un utilisateur oublie son code PIN ou perd l'accès à son compte, il doit suivre une procédure de récupération qui inclut une vérification d’identité stricte pour rétablir l’accès. | **-Limites de transfert** :  Un utilisateur peut transférer un montant limité par jour ou par mois en fonction de son type de compte (compte standard ou vérifié).  Des plafonds spécifiques sont définis pour éviter le blanchiment d’argent et les activités illégales.  **-Frais de transaction** :  Les transferts entre utilisateurs Wave peuvent être gratuits ou soumis à une petite commission, notamment pour les transferts internationaux ou au-delà d'un certain montant.  **-Vérification de l’identité**: Avant tout transfert d’un montant élevé, une vérification d’identité via un code PIN ou une méthode d’authentification à deux facteurs (2FA) est requise.  **-Temps de traitement** :  Les transferts d’argent entre utilisateurs Wave sont généralement instantanés, mais des retards peuvent survenir pour des transferts internationaux ou ceux nécessitant une vérification supplémentaire. | **-Liaison avec les banques**: Pour lier un compte bancaire à son compte Wave, l’utilisateur doit fournir des informations bancaires précises et valider la liaison via un processus sécurisé (authentification bancaire).  **-Frais de transfert bancaire** : Wave peut facturer des frais pour les transferts entre comptes bancaires et le compte Wave, en fonction des accords avec les banques partenaires.  **-Limites de transfert** :  Des plafonds de transfert entre le compte bancaire et le compte Wave peuvent être imposés pour des raisons de sécurité et de conformité réglementaire (notamment contre le blanchiment d'argent).  **-Délais de traitement** :  Les transferts entre un compte Wave et un compte bancaire peuvent prendre plus de temps que les transferts internes Wave (généralement 1 à 3 jours ouvrables). |
| **RISQUE** | **-Risque d'échec de transaction** : Les paiements aux commerçants ou aux services publics peuvent échouer en raison de problèmes de connectivité réseau, de bugs logiciels ou de problèmes avec les comptes des fournisseurs.  **-Risque de contestation des paiements** : Les utilisateurs peuvent contester des paiements effectués de manière incorrecte ou frauduleuse, ce qui pourrait mener à des litiges entre Wave, les utilisateurs et les commerçants.  **-Risque de perte de confidentialité** : Si les informations sur les transactions ne sont pas correctement protégées, cela pourrait exposer les utilisateurs à des risques de vol de données personnelles et financières.  **-Risque d'erreur de facturation** :Des erreurs dans les factures des services publics ou des commerçants peuvent entraîner des paiements incorrects et des réclamations des utilisateurs. | **-Risque de fraude de la part des agents** : Certains agents pourraient tenter d’escroquer les utilisateurs en ne créditant pas leurs comptes après des dépôts en espèces ou en facturant des commissions abusives.  **-Risque de gestion de liquidités insuffisantes** : Les agents peuvent manquer de liquidités pour répondre aux demandes de retrait des utilisateurs, ce qui pourrait causer des interruptions de service et une perte de confiance dans le système.  **-Risque de manipulation des transactions** : Si les agents ne respectent pas les protocoles de sécurité, des erreurs ou des fraudes pourraient survenir, comme des transactions falsifiées ou non enregistrées correctement.  **-Risque de conformité légale**: Les agents peuvent enfreindre les lois locales s’ils ne respectent pas les régulations financières concernant la lutte contre le blanchiment d’argent ou le financement du terrorisme. | **-Risque de piratage de comptes** : Si le code PIN ou les données d’authentification des utilisateurs sont compromis, des tiers malveillants pourraient accéder à leurs comptes et effectuer des transactions frauduleuses.  **-Risque de perte de données**: En cas de défaillance technique ou d’attaque informatique, les informations sensibles des utilisateurs (historique des transactions, informations personnelles) pourraient être perdues ou corrompues.  **-Risque d'erreurs dans la récupération des comptes** :  Des erreurs dans la procédure de récupération de compte (ex : perte de code PIN) pourraient bloquer les utilisateurs légitimes hors de leurs comptes, ou permettre à des fraudeurs d’accéder à un compte à leur place.  **-Risque d'interruption de service** : Une cyberattaque (ex : attaque par déni de service) pourrait paralyser le système et empêcher les utilisateurs d'accéder à leurs comptes ou d'effectuer des transactions. | **-Risque de fraude et de phishing** : Les utilisateurs peuvent être victimes de tentatives de phishing ou de fraude via des messages ou appels frauduleux les incitant à partager leur code PIN ou d'autres informations sensibles.  **-Risque d'erreur humaine**:  Les utilisateurs peuvent envoyer des fonds à une mauvaise personne en raison d'erreurs de saisie (mauvais numéro de téléphone ou identifiant utilisateur).  **-Risque de non-conformité réglementaire** :  Si des montants élevés sont transférés sans vérifications appropriées, Wave pourrait être exposé à des sanctions pour non-respect des réglementations sur le blanchiment d'argent.  **-Risque de surcharge du système** :  Une forte demande lors de périodes spécifiques (ex : jours de paie) pourrait provoquer des retards dans les transferts d'argent, créant des frustrations chez les utilisateurs. | **-Risque de défaillance bancaire** : Si la banque partenaire rencontre des problèmes techniques ou de liquidité, cela pourrait empêcher les utilisateurs de transférer de l’argent entre leur compte bancaire et leur compte Wave.  **-Risque de non-conformité aux normes bancaires** : Wave doit respecter les régulations locales et internationales concernant les transferts d’argent, et tout manquement pourrait entraîner des sanctions ou des interruptions de service.  **-Risque de fraude par intégration bancaire** :  Des erreurs dans la liaison entre un compte bancaire et un compte Wave pourraient permettre à des fraudeurs de détourner des fonds depuis un compte non autorisé.  **-Risque de retard de traitement des transactions** :  Les transferts entre Wave et les comptes bancaires peuvent être sujets à des délais prolongés, ce qui pourrait causer des frustrations chez les utilisateurs, notamment en cas d'urgence. |
| **OPPORTUNITE** |  |  |  |  |  |
| **INDICATEUR** |  |  |  |  |  |
| **INTEGRATION AVEC UN SYSTEME EXTERIEUR** |  |  |  |  |  |