Nexium

Jean HERAIL
jean.herail@epita.fr

Milo DELBOS
milo.delbos@epita.fr

Antonin BESSIÈRES
antonin.bessieres@epita.fr

William VALENDUC
william.valenduc@epita.fr

December 11, 2024

Sommaire

1 Introduction

Nexium serait une économie virtuelle décentralisée conçue pour les étudiants d'Épita. Chaque participant disposerait d'une paire de clés cryptographiques (privée et publique) associée à son adresse `@epita.fr`, permettant d'authentifier et de sécuriser les transactions de crédits entre utilisateurs. Grâce à une architecture distribuée, Nexium garantierait la transparence et l'intégrité des virements tout en offrant une expérience simple et accessible. La monnaie du réseau Nexium, le `NXM`, serait utilisée pour effectuer des transactions entre les utilisateurs, qui pourraient consulter leur solde et leur historique de transactions via une interface graphique intuitive.

Le réseau Nexium s'articule donc comme une blockchain privée, où chaque utilisateur est un noeud du réseau. Chaque bloc, contenant un type d'information unique (création de compte, virement, etc.), sera signé par l'émetteur de la transaction et validé par les autres utilisateurs du réseau. Les soldes des utilisateurs seraient stockés dans une base de données distribuée, garantissant ainsi la cohérence des données et la résilience du système. Les transactions seraient signées par les clés privées des émetteurs et vérifiées par les clés publiques correspondantes, assurant ainsi la sécurité et l'intégrité des échanges.

2 Description du Projet

2.1 Fonctionnalités

- **Création de Comptes** : Les étudiants d'Épita pourront créer un compte Nexium en fournissant leur adresse d'étudiant. Après avoir généré une paire de clés, ils auront à copier la clé publique renvoyée par le programme sur l'interface du Gitlab de l'école, dans le champ des clés GPG . Il s'agira d'une **clé RSA** de 2048 bits. Lors de la création du compte, un solde initial de `1000 NXM` sera attribué à 'utilisateur.

- **Virements** : Les utilisateurs pourront effectuer des virements de crédits entre eux en utilisant leur adresse, les transactions étant signées par la clé privée de l'émetteur et vérifiées par la clé publique correspondante. Les soldes seraient ensuite mis à jour en temps réel et stockés dans une base de données distribuée. Les utilisateurs pourront associer, à chaque transaction, un descriptif optionnel d'une longueur maximale de 140 caractères.

- **Historique des Transactions** : Les utilisateurs pourraient consulter l'historique de leurs transactions, incluant les montants, les dates et les adresses des émetteurs et des récepteurs. Cette transparence est le prix à payer pour une décentralisation de la monnaie.

- **Sécurité** : Le stockage des clés privées se ferait en priorité via des solutions locales matérielles si disponibles, comme un module TPM ou une carte à puce. Cette implémentation nécessitera la communication avec une API système pour accéder à ces dispositifs. En l'absence de telles solutions, les clés privées pourront être chiffrées et stockées localement sur le disque dur de l'utilisateur. Un mot de passe sera alors demandé à chaque transaction pour déchiffrer la clé privée. Ce mot de passe sera initialisé lors de la création du compte et pourra être modifié par la suite.

- **Interface Graphique** : Une interface graphique simple et intuitive permettrait aux utilisateurs de consulter leur solde, d'effectuer des virements et de consulter l'historique de leurs transactions. Elle serait développée avec GTK via Glade.

- *(Facultatif)* **Synchronisation avec les serveurs Forge** : Les soldes et transactions pourraient être certifiés par les serveurs Forge d'Épita, garantissant ainsi l'intégrité des données et la **non-répudiation** des transactions. Ces noeuds de confiance pourraient être utilisés pour vérifier les soldes et les transactions des utilisateurs, en cas de litige ou de perte de données.

3 Annexe

3.1 Définitions

Clé RSA : Clé cryptographique utilisée pour chiffrer et déchiffrer des données. Elle est composée d'une paire de clés, une publique et une privée, qui sont générées simultanément. La clé publique est utilisée pour chiffrer les données tandis que la clé privée est utilisée pour les déchiffrer.

Non-répudiation : Obligation de ne pas pouvoir nier un acte ou une transaction. En cryptographie, la non-répudiation est la propriété qui permet de prouver qu'une transaction a bien été effectuée par une entité donnée.