haute école neuchâtel berne jura arc ingénierie www.he-arc.ch

Hes·so Haute Ecole Spécialisée de Suisse occidentale

Blockchain based privacy

Alexis PORTMANN

Travail de bachelor 2021

Informatique - Développement Logiciel et Multimédia

Professeur: Ninoslav MARINA

Expert: Dr. Ania Piotrowska

Description

Nym est une entreprise basée à Neuchâtel qui se spécialise dans les techniques du blockchain, de la cryptographie et de la communication. Elle a pour but d'offrir une solution permettant de communiquer de façon anonyme, sécurisée et résiliente à tout type d'adversaires. Cette solution se veut adoptable dans la majorité des domaines d'application qui utilisent internet. Pour ce faire, elle implémente un réseau décentralisé qui allie différentes technologies de cryptographie et de communication.

Dans le cadre de ce travail de bachelor, il a été demandé à l'étudiant d'implémenter une solution permettant de déployer le réseau Nym sur une machine locale, afin de pouvoirs tester ses vulnérabilités ainsi que de potentielles améliorations sans devoir le déployer sur un réseau physique de test entièrement dédié.

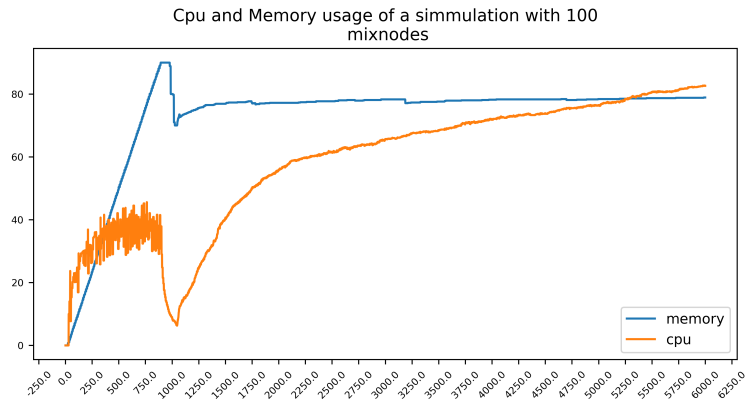
Déroulement

Ce travail a été réalisé en trois phases :

- Familiarisation avec les techniques utilisées : Les logiciels de Nym sont développés à Rust et en Go, ils utilisent des protocoles d'encryptage et de routage.
- L'exploration des solutions possibles : Le simulateur doit partiellement isoler les logiciels de la machine hôte, ce qui peut être fait à plusieurs niveaux. (VM, redirection de flux, etc.).
- L'implémentation du simulateur locale

Résultats

Un simulateur fonctionnel permettant de déployer un réseau de taille variable a été obtenu. Il est simple et rapide à déployer, et permet de facilement mesurer la consommation des ressources et le flux de données. Cela permet d'analyser l'impact de différents scénarios sur le réseau et de pouvoir tester les nouvelles fonctionnalités des différents logiciels avant de les déployer sur le vrai réseau.



Utilisation cpu et mémoire cumulée de 100 mixnodes déployés à la chaine

La figure ci-dessus montre la consommation de ressources de 100 instances d'une composante du réseau Nym déployée sur le simulateur.

En connaissant la configuration de la machine qui l'a fait tourner, elle donne aussi un ordre de grandeur aux ressources qu'il faudrait réquisitionner pour simuler des réseaux à plus grande échelle.

Perspectives

Ce simulateur offre aux développeurs de Nym la possibilité de pouvoir tester les nouvelles fonctionnalités de leurs logiciels sans s'encombrer d'un réseau physique composé de plusieurs machines.
Il permet aussi de faire des simulations d'instances à grande échelle du réseau, ce qui serait trop onéreux avec des machines physiques.