TELECOM Nancy - 1A par apprentissage
Projet PPII 2021 : TNcoin

1 Description générale

Le projet PPII a pour objectif de vous faire appliquer au sein d'un même projet les différentes connaissances acquises en STIC durant le S6 de la formation, à savoir en langage C, en web et bases de données, et en réseau. Le projet consiste cette année à réaliser une blockchain "TNcoin" permettant l'échange de crypto-actifs et similaire à Bitcoin.
Cette année, l'objectif du projet et de pouvoir émettre des transactions à partir d'un site web gérant les wallets et que celles-ci soient validées et stockées dans votre blockchain tel qu'illustré dans la figure 1.

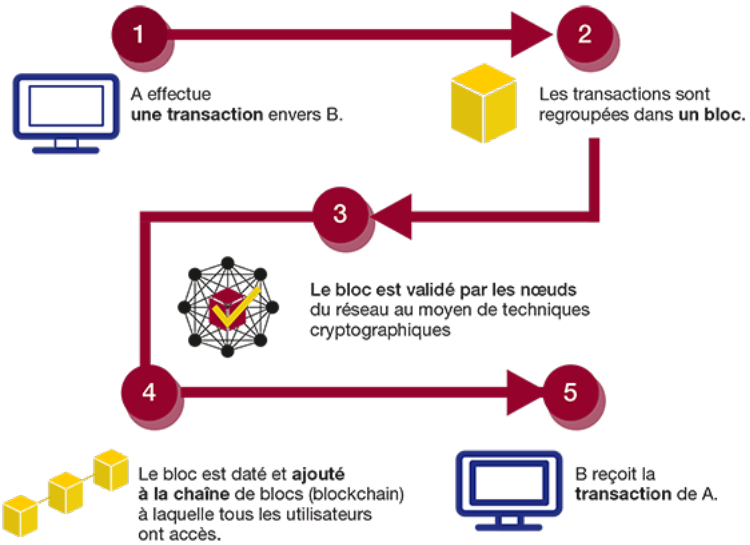

FIGURE 1 – Étapes de validation d'une transaction [source : coin24]

Le projet comporte quatre grandes parties, une étude bibliographique, une phase de conception, la réalisation de la blockchain et la réalisation du site web gérant les wallets.
La blockchain elle même doit fonctionner sur le même modèle de réseau pair à pair que Bitcoin, regrouper les transactions en blocs tel qu'illustré dans la figure 2. Ces blocs sont ensuite validés avec le système de "proof of work" utilisé par Bitcoin. Vous devrez viser un débit moyen d'un bloc par minute selon la puissance de calcul disponible des "miners" du réseau, sans oublier de les rémunérer en TNcoins une fois le bloc créé. Vous supposerez qu'une "Initial Coin Offering" a eu lieu et initialisez la blockchain avec un certain nombre de blocs.
Le site de gestion des wallets doit vous permettre de créer un compte, de visualiser les informations qui y sont associées, de passer des transactions avec d'autres utilisateurs. Pour éviter de consulter la blockchain à chaque sollicitation, le site web de gestion des wallets utilisera sa propre base de données relationnelle localement. Le backend du site interagira avec la blockchain pour passer les transactions.

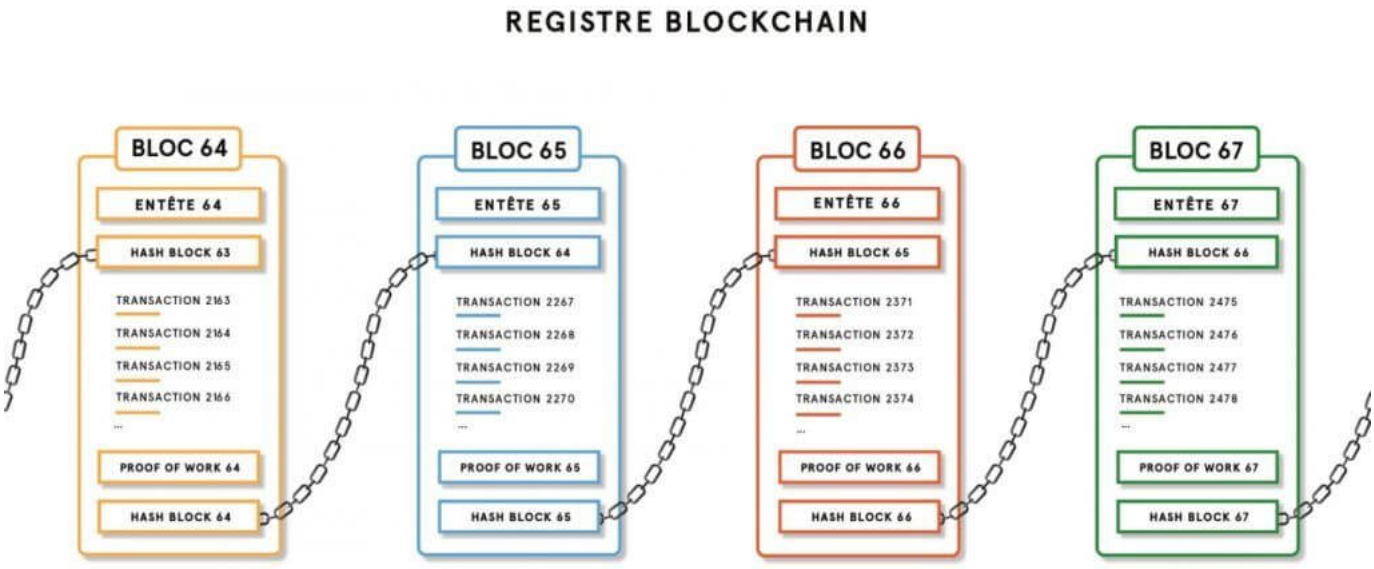

FIGURE 2 – Structure d'une chaîne de blocs [source : coin24]

2 Travail attendu

2.1 Étude bibliographique et conception

Vous réaliserez dans un premier temps une étude bibliographique vous permettant de monter en compétence sur les principaux mécanismes mis en œuvre par Bitcoin. La littérature est très abondante sur le sujet et il vous revient de trouver des sources pertinentes, éventuellement de les croiser, et de rendre compte des connaissances que vous en aurez tirées dans le rapport, tout en veillant bien à citer les documents qui vous ont servi. Pour commencer, le white paper de Bitcoin est incontournable. De même, le wiki de la communauté est une mine d'information. Vous devrez en particulier étudier les structures de données "merkle trees" utilisées dans les blocs, le fonctionnement du "proof of work", et les communications entre les pairs.
La partie conception doit vous permettre d'anticiper la plupart des questions fonctionnelles ou techniques avant de toucher au code. Cette partie contiendra deux sous-parties dédiées respectivement aux spécifications fonctionnelles et aux spécification techniques. Les spécifications fonctionnelles doivent décrire les fonctionnalités de l'application à travers des cas d'utilisation. Les spécifications techniques décriront les mécanismes dont vous avez besoin et leurs interactions : architecture de l'application, principales structures de données, schéma de la base de donnée, protocole de communication, algorithmes, etc. Les interactions sont typiquement modélisées par des diagrammes de séquences. Quand cela est pertinent, une estimation de la complexité est à faire.

2.2 Réalisation et validation

La blockchain sera réalisée en langage C. Une interface graphique n'est pas demandée pour cette partie. Le site web utilisera Postgresql pour la base de données et le langage vu dans le module Webdb pour la partie web dynamique. Tout le code que vous réaliserez devra être versionné sur la plateforme gitlab de l'école, chacun doit commiter avec son propre compte. Dans le rapport, vous justifierai les choix techniques faits pour implanter les différentes fonctionnalités et mentionnerez les difficultés éventuelles.
Enfin, vous devrez justifier des résultats obtenus dans une dernière partie d'évaluation. Vous détaillerez les tests réalisés (tests unitaires, d'intégration, fonctionnels) et illustrerez le fonctionnement de vos applications.

Vous testerez notamment les différents cas limites et évaluerez les performances de la blockchain quand de nombreuses transactions sont générées (par des programmes de tests).

3 Rendu

Le projet se fait en trinôme (groupes libres) et sera évalué sur la base d'un rapport (à rendre pour le 02/06), d'une soutenance (le 09/06) et bien entendu du code produit et versionné sur le Gitlab de l'école.
Vous réaliserez un Makefile permettant la génération de l'exécutable et un fichier README donnant les indications pour l'exécution.
Le rapport devra notamment contenir :

- une étude bibliographique de la blockchain de Bitcoin ;
- une description des principaux cas d'utilisation identifié ;
- des éléments de conception technique, notamment :
  - les structures de données utilisées ;
  - le protocole applicatif (type et format des messages) entre pairs ;
  - l'algorithme d'un noeud Bitcoin ;
  - le schéma de la base de données du site web ;
  - les interactions entre les composants ;
- l'implantation des différents composants et les difficultés techniques éventuelles ;
- les tests effectués pour valider votre développement et en garantir la qualité ;
- la répartition du travail entre les membres du groupes et aures éléments de gestion de projet que vous jugerez pertinents.