Projet S4

Cahier des charges

Groupe TREG

CAVALIÉ Margaux
LITOUX Pierre
PINGARD Adrien
RUIZ Hugo
VEYRE Thimot

Encadrant : VERNAY Rémi

TABLES DES MATIÈRES

Introduction

Ce cahier des charges présente notre projet de S4, un logiciel dans lequel l'algorithmique occupe une part très importante. Le sujet est libre, et encadré par le docteur en informatique et expert auprès de la cour d'appel de Toulouse Rémi Vernay. Le projet sera développé sous Linux, et codé en langage C.

Ce cahier contient une présentation générale du projet, en plus de la répartition des tâches et du planning détaillé de réalisation. Notre groupe est actuellement constitué de 5 personnes : Cavalié Margaux, Litoux Pierre, Pingard Adrien, Ruiz Hugo et Veyre Thimot. Il est fort probable que Pierre Litoux parte en séjour à l'international, c'est pourquoi nous sommes un groupe de cinq personnes, et non quatre comme le prévoit le sujet.

Pour notre projet, nous avons choisi de recréer la technologie d'une blockchain. Cette technologie est décrite pour la première fois dès 1991 par les chercheurs Stuart Haber et W. Scott Stornetta, qui cherchaient à horodater des documents numériques pour que ceux-ci ne soient jamais antidatés ou altérés. Cette technologie tombera dans l'oubli, et perdra son brevet en 2004, quatre ans avant la création du Bitcoin.

En 2004, un activiste cryptographique, Hal Finney, lance le système appelé "preuve de travail réutilisable", qui permet de conserver le registre de propriété des informations envoyées pour permettre à n'importe quel utilisateur du réseau de vérifier l'exactitude et l'intégrité des données en temps réel. Ce n'est qu'en 2008 que Satoshi Nakamoto fait naître le Bitcoin en reliant ces deux technologies. Il envoya dix Bitcoins à Hal Finney, et offrit cinquante Bitcoins de récompense à celui qui minerait le bloc. Le Bitcoin et la Blockchain comme nous les connaissons sont ainsi créés.

L'objectif de notre projet est de récréer cette technologie. Pour cela, il nous faudra nous intéresser à la cryptographie et à la création d'un réseau qui mettrait en relation tous les différents utilisateurs. Le dernier rendu du projet est prévu pour la semaine du 14 juin 2021, nous avons ainsi trois mois et demi pour porter notre projet à terme.

État de l'art

Fonctionnement de la blockchain

Le terme blockchain (ou chaîne de blocs) désigne la technologie de consensus décentralisé. La blockchain est donc une technologie de stockage et de transmission d'informations, transparente, sécurisée, fonctionnant sans organe central de contrôle.

Toute blockchain publique fonctionne nécessairement avec une monnaie ou un jeton programmable. Les transactions effectuées entre les utilisateurs du réseau sont regroupées par blocs.
Avant d'être approuvé, chaque bloc est validé par les nœuds du réseau (appelés les "mineurs"), selon des techniques qui dépendent du type de blockchain. Dans la blockchain du bitcoin cette technique est appelée le "Proof-of-Work" (preuve de travail), et consiste en la résolution de problèmes algorithmiques.
Une fois le bloc validé, il est horodaté et ajouté à la chaîne de blocs. La transaction est alors visible pour le récepteur et pour l'ensemble du réseau. Au cours du temps, des blocs sont ajoutés à la chaîne. Une blockchain publique est donc comparable à un grand livre comptable public : anonyme et infalsifiable.

A l'inverse, une blockchain privée est contrôlée par une entité totalement centralisée dans le réseau, et les membres participants doivent avoir été acceptés et déclarés par cette entité. Les transactions peuvent être émises par chacun des nœuds, mais elles sont validées et ajoutées à la chaîne par le nœud central autorisé à le faire. Il n'existe aucun mécanisme de consensus, et les règles de fonctionnement sont spécifiques au dispositif et aux accords passés par les membres de la communauté d'utilisateurs.

La blockchain contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est sécurisée et distribuée, c'est-à-dire qu'elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne.

Ce qui rend la blockchain si fiable et sécurisée, c'est l'ensemble des méthodes qui permettent aux participants du réseau distribué de se mettre d'accord, sans recourir à un tiers de confiance.

Il existe actuellement deux grandes familles de blockchain. Leur différence réside dans la manière dont les blocs sont validés. La première est la validation par “preuve de travail” (proof of work), et la deuxième la validation par “preuve d’enjeu” (proof of stake).

Validation par proof of work

La validation par preuve de travail est la plus simple à mettre en place. En effet, dans ce système les mineurs doivent résoudre un problème mathématiques très complexe, plus le nombre de mineurs augmente, plus cette complexité augmente également, pour valider un bloc. Ce problème dépend du bloc précédent, de cette manière pour modifier un bloc donné dans la chaîne, il faut également recalculer tous les blocs suivants.

Cette méthode de validation à l'inconvénient majeur d’être extrêmement énergivore et pose un gros problème environnemental.

Validation par proof of stake

Le deuxième principe de validation est la preuve d’enjeu. Cette méthode choisit un ou plusieurs mineurs parmi ceux disponibles et ceux-ci valident le bloc sans calcul complexe. Les mineurs sélectionnés peuvent être choisis selon plusieurs critères (leur ancienneté, leur quantité de monnaie, etc). Ce système permet de réduire grandement la consommation énergétique lié au minage mais il a l'inconvénient majeur d’être de ce fait un peu moins sécurisé

Ces méthodes, pour fonctionner à grande échelle, doivent être rémunérées pour que le réseau continue à fonctionner. En effet, les membres du réseau doivent pouvoir rentabiliser les dépenses liées aux vérifications.

Notre projet

Notre cryptomonnaie utilisera deux familles d'acteurs pour fonctionner.
Les premiers sont les nœuds de gestion, qui s'occupent de recevoir les transactions et de créer les blocs. Les seconds sont les nœuds de minages, qui sont appelés par les nœuds de gestion pour résoudre un problème mathématique permettant de sécuriser la blockchain.
Les nœuds de gestion devront intégrer des sécurités permettant d'éviter la création de blocs malicieux.

Le réseau devra être constitué d'au minimum un nœud de gestion et un nœud de minage. Même si cela implique de gros problèmes de sécurité, nous souhaitons que ce soit possible car c'est un projet, et que le réseau ne sera constitué que de quelques ordinateurs de confiance lors de nos tests.

Pour le système de validation, nous avons décidé de nous orienter vers la validation "proof of work", qui nous semble plus simple à implémenter. Étant donné que le projet restera à petite échelle, l'impact environnemental sera minime. Néanmoins, s'il venait à prendre de l'importance, il nous faudrait le faire fonctionner en "proof of stack" pour réduire son impact énergétique.

La blockchain permet de stocker et transmettre des données, mais les utilisateurs de celle-ci auront besoin d'une interface pour réaliser leurs transactions et consulter l'historique des transactions déjà réalisées. Comme pour la blockchain du Bitcoin, il nous faudra un site ou toutes ces informations sont accessibles en quelque clic , il devra donc intégrer une gestion de compte ou chaque utilisateur aura accès à ses données personnelles tel que visualiser le solde du compte et réaliser des transactions avec les autres utilisateurs. Un site avec une certaine sécurité devra alors être mis en place pour éviter que d'autres personnes y accèdent de façon illégitime et détourne nos fonds.

Nous coderons notre site en HTML5 et CSS, puis nous utiliserons le certificat HTTPS pour garantir aux utilisateurs la confidentialité et l'intégrité de leur données lorsqu'ils en envoient ou en reçoivent. Les utilisateurs pourront ainsi créer leur compte et obtenir un portefeuille qui leur permettra d'échanger des données avec les autres utilisateurs du réseau en toute sécurité.

Planning

Répartition des tâches

	Réseau	Noeud de minage	Noeud de gestion	Site web
Margaux		⊕		+
Pierre	+	+	+	
Adrien			⊕	
Hugo	+			⊕
Thimot	⊕			

Légende :

⊕ → Responsable

\+ → Suppléant

Planning détaillé de réalisation

Première soutenance

Réseau :

- Simulation d'un réseau en multi-thread
- Exécution des différent noeuds sur différents process
- Début de mise en réseau sur plusieurs machines

Site web :

- Ébauche de site web

Noeuds :

- Début du noeud de gestion
- Fonction de hash primaire et minage brute force
- Interaction noeud de minage/noeud de gestion primaire

Deuxième soutenance

Réseau :

- Réseau capable de fonctionner sur plusieurs machines

Site web :

- Amélioration de l'esthétique du site
- Possibilité d'utiliser notre blockchain depuis le site

Noeuds :

- Validation des blocs par la majorité des noeud de gestion
- Complexité du hash régulée automatiquement en fonction de la puissance de calcul

Soutenance finale

Réseau :

- Réseau fiable

Site web :

- Site web esthétiquement abouti
- Site web sécurisé
- Système de compte et de connexion sur le site

Noeuds :

- Résolution des derniers problèmes de décentralisation de certaines données dans les noeuds de gestion

Conclusion

Nous sommes tous prêts à relever le défi que représente l'implémentation d'une blockchain, et à nous investir dans un travail de groupe qui se veut assez conséquent. La difficulté de ce projet réside dans la mise en relations des différents éléments qui composent une blockchain, avec la gestion de la sécurité et la décentralisation des données, afin de garantir la confidentialité des transactions et de l'utilisateur lui-même au sein du réseau.