




Présentation SecuraChain - SAÉ S5

👤 Owner	 Pierre Leocadie
☰ Tags	Document Information SecuraChain
🕒 Last edited by	👤 Jordan Dohou

ÉQUIPE :

Jordan DOHOU

Ulrich SCHMITH

Pierre LEOCADIE

François PEUCH

Sathusan KRISHNAPAKARAN

Allan HERILUS



Professeur référent : Jean-François
BRETTE

Groupe 306

▼ Sujet

Concevoir et mettre en œuvre une blockchain décentralisée pour le stockage sécurisé et la gestion des données.

Nous avons entrepris un projet passionnant qui consiste à créer une technologie basée sur une blockchain, semblable à celle qui sous-tend les cryptomonnaies telles que le Bitcoin, mais avec un objectif différent. Imaginez un monde où vous pouvez stocker vos données personnelles, qu'il s'agisse de photos, de documents, de vidéos, ou d'autres informations importantes, en toute sécurité, sans avoir à faire confiance à une seule entreprise ou une autorité centrale pour les protéger. C'est

l'objectif de notre projet ambitieux : concevoir et mettre en œuvre une blockchain décentralisée dédiée au stockage sécurisé et à la gestion transparente des données.

▼ Pourquoi ce sujet ? Une réponse en 8 points clés

1. **Exploration de la technologie blockchain** : La blockchain est une technologie innovante et en pleine expansion qui a le potentiel de transformer divers secteurs, y compris la sécurité et la gestion des données. En explorant la création d'une blockchain, nous aurons l'opportunité de plonger au cœur de cette technologie émergente et de comprendre son fonctionnement en profondeur.
2. **Développement de compétences techniques** : La mise en œuvre d'une blockchain exige des compétences techniques avancées en matière de développement logiciel, de cryptographie et de sécurité informatique. Ce projet nous permettra de développer nos compétences dans ces domaines, ce qui sera précieux pour notre future carrière en tant que professionnels de la sécurité et des réseaux.
3. **Gestion des données et sécurité** : En tant qu'étudiants en sécurité, nous comprenons l'importance de la gestion sécurisée des données. La blockchain offre des mécanismes de sécurité intégrés, et ce projet nous donnera l'occasion d'explorer comment ces mécanismes peuvent être utilisés pour garantir la confidentialité, l'intégrité et l'authenticité des données.
4. **Décentralisation et réseaux** : Le sujet met en avant le concept de décentralisation, qui est un aspect clé des blockchains. En tant qu'étudiants en réseaux, nous aurons l'occasion de comprendre comment les nœuds d'un réseau blockchain interagissent et coopèrent pour atteindre un consensus, tout en maintenant la décentralisation.
5. **Application pratique de la cryptographie** : La cryptographie est au cœur de la sécurité des blockchains. Ce projet nous permettra d'appliquer des concepts de cryptographie tels que la création de paires de clés, le chiffrement et la signature numérique dans un contexte pratique.
6. **Collaboration en équipe** : En tant que groupe de six étudiants, nous aurons l'occasion de travailler en équipe sur un projet complexe. Cela reflète

également la réalité de nombreux projets en informatique, où la collaboration est essentielle.

7. **Réponse aux besoins actuels** : La gestion sécurisée des données est une préoccupation majeure dans le monde moderne. La capacité à concevoir et à mettre en œuvre une blockchain pour répondre à ces besoins est pertinente et offre une expérience pratique dans un domaine en demande.
8. **Préparation à l'industrie** : La blockchain est de plus en plus adoptée par l'industrie, y compris dans des domaines tels que les finances, la santé et la logistique. En acquérant des compétences dans ce domaine, nous nous préparons à des opportunités de carrière prometteuses.

En résumé, ce projet combine plusieurs aspects essentiels de notre formation, notamment la sécurité informatique, les réseaux et le développement logiciel, tout en explorant une technologie de pointe. Il offre une opportunité passionnante d'apprentissage et de développement de compétences, tout en nous permettant de contribuer à la résolution de problèmes concrets liés à la sécurité et à la gestion des données.

▼ Les grandes étapes du sujet (Lot 1)

1. Comprendre le fonctionnement d'une blockchain :

- Il s'agit essentiellement d'une base de données distribuée, où chaque participant du réseau (nœud) possède une copie de cette base de données. Les données sont regroupées en blocs et ajoutées de manière sécurisée à la chaîne existante. Chaque bloc est lié au précédent, créant ainsi une chaîne de confiance.
- Étudier en détail le fonctionnement des blockchains, y compris les concepts de base tels que les blocs, la chaîne, la décentralisation et le consensus. Cela nous donnera une base solide pour concevoir notre blockchain.

2. Définir les différents rôles des nœuds :

- Pour que notre blockchain fonctionne correctement, nous devons définir les rôles que chaque nœud jouera. Par exemple, certains nœuds pourraient être responsables du stockage des données, tandis que

d'autres valideront les transactions et veilleront à ce que les règles du réseau soient respectées.

- Identifier les rôles spécifiques que les nœuds joueront dans notre réseau de blockchain. Par exemple, les nœuds de stockage, nœuds de validation, nœuds de contrôle, etc.

3. Choisir un mécanisme de consensus :

- Le consensus est la manière dont les nœuds du réseau s'accordent sur l'état de la blockchain. Des mécanismes comme la preuve de travail (PoW) ou la preuve d'enjeu (PoS) sont utilisés pour assurer que tous les nœuds sont d'accord sur l'ajout de nouveaux blocs.
- Sélectionner le mécanisme de consensus qui convient le mieux à notre blockchain. Chaque mécanisme a ses avantages et ses inconvénients.

4. Définir le protocole de communication :

- Les nœuds doivent communiquer entre eux pour maintenir la synchronisation de la blockchain. Nous devons développer un protocole de communication qui permettra aux nœuds de partager des données de manière sécurisée.
- Créer un protocole de communication clair et standardisé que les nœuds utiliseront pour interagir entre eux. Cela peut inclure des spécifications sur la manière dont les données sont transmises, comment les nœuds se synchronisent, etc.

5. Gestion des interactions entre les nœuds :

- Définir les scénarios dans lesquels les nœuds interagiront entre eux. Par exemple, comment les nœuds de stockage recevront-ils des données des utilisateurs, comment les nœuds de validation vérifieront-ils les transactions, etc.

6. Structure des blocs :

- Concevoir la structure des blocs de notre blockchain, y compris la manière dont les transactions seront stockées à l'intérieur. Nous devons également décider de la fréquence à laquelle de nouveaux blocs sont

créés. Par exemple, comment ajouter, modifier ou supprimer des données sur la blockchain.

7. Gestion des transactions :

- Définir les actions spécifiques qui peuvent être effectuées sur notre blockchain, telles que l'ajout de fichiers, la modification, la suppression, etc. Créer des règles pour la gestion de ces transactions.

8. Gestion des clés et de la sécurité :

- Les clés privées sont essentielles pour accéder aux données. Nous devons concevoir des méthodes robustes de gestion des clés pour protéger les données des utilisateurs.
- Élaborer des mécanismes de gestion des clés pour assurer la sécurité des données stockées sur la blockchain. Considérer la manière dont les utilisateurs créeront et protégeront leurs clés privées.

▼ Conception d'une application basée sur notre blockchain (Lot 2 - Si on a le temps)

1. Concevoir l'Architecture :

- Définir l'architecture générale de l'application. Décider si elle sera basée sur le Web, une application de bureau ou une application mobile. Choisir également la technologie de développement appropriée en fonction de nos compétences et de nos besoins.

2. Conception de l'Interface Utilisateur (UI) :

- Créer des wireframes et des maquettes pour concevoir l'interface utilisateur. Penser à l'agencement des éléments, à la navigation, aux icônes, aux couleurs et à l'esthétique générale. Nous nous assurerons également que l'interface soit intuitive et conviviale.

3. Développement Front-End :

- Commencer à développer le front-end de l'application en utilisant des technologies telles que HTML, CSS et JavaScript. Intégrer les fonctionnalités nécessaires pour interagir avec la blockchain, telles que la gestion de clés, l'envoi de transactions, etc.

4. Connexion à la Blockchain :

- Mettre en place une connexion entre l'interface utilisateur et notre blockchain en utilisant une API.

5. Gestion de Comptes Utilisateurs :

- Créer des mécanismes de gestion des comptes utilisateurs, y compris la génération de paires de clés, la gestion de l'identité de l'utilisateur et la sécurité des comptes.

6. Intégration de Fonctionnalités :

- Ajouter des fonctionnalités telles que la visualisation des transactions, la consultation de l'historique, l'ajout de données à la blockchain, la recherche, etc.

7. Sécurité :

- Mettre en œuvre des mesures de sécurité robustes pour protéger les comptes des utilisateurs et les données stockées sur la blockchain.

8. Déploiement :

- Déployer l'application sur un serveur ou une plateforme en fonction de notre choix d'architecture. S'assurer qu'elle est accessible aux utilisateurs.

▼ Inspiration

Nous pouvons nous inspirer de deux technologies open source : la blockchain Storj, qui est disponible sur GitHub et a été programmée en Go, et le protocole IPFS, développé en Go, également disponible en open source.

▼ Stack technique

- Go (Golang)
- Docker
- Git/Github
- AWS

▼ Compétences visées

1. Connaissance approfondie de la blockchain :

- Comprendre en profondeur le fonctionnement des blockchains, les principes de décentralisation, de consensus et de sécurité.

2. Compétences en cryptographie :

- Apprendre à utiliser la cryptographie pour sécuriser les données et les transactions sur la blockchain.

3. Réseaux et sécurité :

- Appliquer les connaissances en réseaux et en sécurité pour garantir la robustesse et la sécurité de la blockchain.

4. Développement de logiciels :

- Compétences en développement de logiciels pour la mise en œuvre pratique de la blockchain, en utilisant Go (Golang).

5. Gestion de projet :

- Acquérir des compétences en gestion de projet pour planifier, organiser et exécuter efficacement un projet complexe en équipe.

6. Travail d'équipe :

- Développer des compétences en travail d'équipe en collaborant avec d'autres étudiants pour atteindre des objectifs communs.

7. Analyse de problèmes complexes :

- La capacité à analyser et à résoudre des problèmes complexes liés à la blockchain et à l'architecture décentralisée.