Cheikh Anta Diop **Ecole Supérieure**

Polytechnique Dakar

Département Génie Informatique

Blockchain

Année Universitaire 2021-2022

Projet sur blockchain avec CORDA

Présenté par : ***Groupe 2***

Haby Diop

Mariama ka

Marieme Aidara

Papa Cheikh Gningue

Tamba Bedel Brice Thiombiano

Professeur :

Mr NIANG

Classe : ***Master 2 SRT et Master 2 GLSI***

PLAN

1. INTRODUCTION

1.1 RÉSUMÉ DU CONTEXTE DE TRAVAIL

Ce contexte nous oriente sur les problèmes que rencontre la population dans le domaine de légitimé des terres qui doit être cadré par le **foncier**. Ces problèmes sur les terres au Sénégal sont causés par la non déclaration de certaines terres sur les registres d'immatriculation (sachant qu'il y'a des terres au Sénégal qui n'appartiennent ni à l'Etat ni des personnes lambda et que des malhonnêtes peuvent s'approprier et l'utiliser à leurs guise). Donc il y a un fort manque de sécurité si on veut acheter des terres légales.

Pour régler ce problème de sécurité on va essayer de **digitaliser** le système d'administration frontière fiable qui va fournir une meilleure sécurité et pourrait assister à la sauvegarde des droits de toute partie prenante en cas de comportement malhonnête sur les terres.

C'est dans ce déroulement de digitalisation de notre système qu'on va créer un système de registre foncier/immobilier basé sur la **blockchain** a émergé.

1.2. DÉFINITION DES TERMES ET OUTILS UTILISÉS

Foncier : Désigne ce qui touche aux terres en tant que fonds c'est-à-dire en tant que richesse ou propriété. L'étude du foncier est l'étude des modes d'appropriation des terres. Ses orientations jouent un rôle essentiel dans toute politique d'aménagement du territoire, dans les modalités du développement tant urbain que rural.

Digitalisation : la digitalisation représente **l'action de numériser**. C'est un anglicisme bien connu, mais aujourd'hui sa définition a évolué. Numériser signifie convertir une information analogique sous forme numérique. Digitaliser, comme tout autre synonyme, s'approche de ce terme.

Blockchain : Mode de stockage et de transmission de données sous forme de blocs liés les uns aux autres et protégés contre toute modification. Dans notre situation, la **blockchain** va permettre de gérer et de signer des contrats ainsi que de vérifier la provenance sur nos transactions de nos terres.

Signature : c'est le graphisme par lequel une personne s'identifie dans un acte et par lequel elle exprime son approbation au contenu de ce document. La validité de tout engagement est subordonnée à l'existence de cette signature manuscrite qui confère au document sa force probatoire.

Signature multiple : Le système fonctionne grâce à l'emploi d'une technologie de cryptographie spécialement conçue à cet effet. On sollicite un dispositif multisignal (signature multiple) lorsqu'on doit obtenir une autorisation collective pour la validation d'une transaction. L'usage d'adresses multi-signatures permet d'améliorer la sécurité informatique liée au paiement et au stockage d'une crypto monnaie. On recourt généralement à deux clefs numériques (une privée, et une seconde publique). Elles peuvent se présenter dans différents formats afin de produire une signature de type multisignal.

Corda : Corda est une plateforme technologique Blockchain conçue pour transformer la façon dont le monde fait des affaires. Grâce aux technologies Smart Contrat et Blockchain, Corda permet aux réseaux d'entreprise existants de réduire les coûts de transaction et de conservation des données et de moderniser leurs opérations commerciales.

2. RÉSUMÉ SUR LES ÉTAPES DE LA TRANSACTION

- ### Gestion de transaction au sein d'une blockchain

La première étape d'une transaction au sein d'une blockChain est l'intégration des informations caractérisant cette transaction (montant transféré, fonds disponibles de l'émetteur, destinataire…) à un bloc. Un bloc regroupe plusieurs transactions.
Pour cela, la transaction doit être validée par plusieurs noeuds du réseau appelés en jargon de la blockchain les « miners » ou mineurs en français. Ces derniers vérifient la conformité de la transaction en résolvant un problème cryptographique complexe et consommateur de puissance informatique (impact énergétique de la Blockchain).
La vérification de cette résolution est faite collectivement grâce à une méthode de validation de bloc appelée « Proof of Work » ou en français preuve de travail. La Proof of Work (PoW) est le résultat du problème cryptographique à résoudre pour qu'une nouvelle

information soit ajoutée dans un bloc. Ce résultat est difficile à obtenir et nécessite beaucoup de puissance informatique. En revanche, sa vérification est peu consommatrice de ressources ce qui peut être effectué par le plus grand nombre. La Proof-of-Stake (preuve d'intérêt) est une autre méthode de validation des blocs. Celle-ci est basée sur les avoirs (ainsi que leur temps de conservation) de la personne et se définit généralement par un pourcentage de création monétaire. C'est une méthode parallèle pour atteindre un consensus décentralisé et qui a l'avantage de consommer peu d'énergie (Peercoin, NeuCoin ou BlackCoin sont des monnaies PoS). Les deux méthodes ne sont pas exclusives et sont parfois utilisées conjointement.
Cette opération s'appelle le « mining » ou minage en français. Une fois que l'ensemble des mineurs s'accordent sur la validité de la « Proof of Work », la transaction est intégrée à un bloc. Celui-ci vient s'ajouter à la chaine de blocs.
Il existe un consensus majoritaire entre les différents acteurs du réseau qui est derrière l'ajout de nouveau blocs. Ce consensus est le vecteur de désintermédiation et il s'incarne par la validation collective de la « Proof of Work » ou « Proof of Stake ».

- ### Les données de transaction

La blockchain Bitcoin est la plus ancienne blockchain. Les blocs de la chaîne de blocs Bitcoin comportent environ 1 Mo de données chacun. Mi-2018, elle comptait environ 525 000 blocs, soit un total d'environ 525 000 Mo stockés dans cette blockchain. Les données de la blockchain Bitcoin existent de façon séparée, en dehors des données de transaction. Celles-ci sont, elles, relatives aux transactions Bitcoin. C'est un registre gigantesque de toutes les transactions Bitcoin ayant eu lieu, depuis la toute première transaction Bitcoin jusqu'à ce jour.

3. ETUDE DES CONCEPTS DE SIGNATURE MULTIPLE

Pour pouvoir envoyer des transactions ou des blocs sur la Blockchain, ils doivent être obligatoirement signés.

Signer une transaction va ajouter une propriété « **Proof** » dans l'objet de cette dite transaction, cette entrée est un simple tableau qui contiendra notre signature, preuve que nous avons bien signé ces données avec notre compte et qui pourrait contenir jusqu'à 7 autres signatures dans le cas d'une transaction Multisig.

6. IMPLEMENTATION & REALISATION

1. Plateforme CORDA

Corda est une plateforme de blockchain open source qui se concentre sur la confidentialité et la sécurité des transactions financières. La multi-signature dans Corda est une fonctionnalité qui permet à plusieurs parties de signer une transaction avant qu'elle ne soit engagée dans la blockchain. Cela ajoute une couche de sécurité supplémentaire à la transaction et garantit que toutes les parties impliquées dans la transaction s'entendent sur ses conditions. Pour implémenter la multi-signature dans Corda, un flux personnalisé peut être développé qui nécessite les signatures de plusieurs parties avant que la transaction puisse être validée dans le grand livre.

2. Les étapes de déroulement sur CORDA

Voici les étapes générales du déroulement d'une plateforme sur Corda :

a. **Définition des participants :** les participants au réseau Corda sont identifiés et leur identité est vérifiée.

b. **Définition des contrats :** les contrats qui régissent les transactions sur le réseau sont définis et codés en utilisant le langage de programmation Kotlin.

c. **Mise en place du réseau :** les nœuds du réseau sont déployés et les participants s'y connectent pour commencer à échanger des données.

d. **Création et envoi de transactions :** les participants peuvent créer et envoyer des transactions entre eux en suivant les contrats définis.

e. **Validation des transactions :** les transactions sont validées par les nœuds du réseau avant d'être enregistrées sur la blockchain.

f. **Stockage des données :** les données sont transférées sur la blockchain de manière sécurisée et peuvent être consultées par les participants autorisés.

g. **Mise à jour des contrats :** les contrats peuvent être mis à jour pour s'adapter aux nouveaux besoins du réseau.

En général, Corda permet une collaboration efficace entre les participants d'un réseau en utilisant des contrats intelligents et en garantissant la sécurité et la confidentialité des données échangées.

3. Approfondissement sur chaque étape de déroulement sur CORDA

a) Définition des participants :

Les participants sur Corda sont des entités qui interagissent sur la plateforme en utilisant des contrats pour gérer des transactions. Les participants peuvent inclure des banques, des entreprises, des gouvernements et d'autres acteurs de l'industrie.

Chaque participant sur Corda dispose d'un nœud sur la plateforme qui lui permet de communiquer avec les autres nœuds et de participer aux transactions. Les participants peuvent ajouter et retirer des contrats de leur nœud, signer des transactions et enregistrer des états sur la chaîne de blocs de Corda.

Les participants sur Corda peuvent également définir des stratégies de confidentialité pour contrôler qui peut accéder à leurs informations de transaction et comment ces informations peuvent être utilisées. Cela permet aux participants de conserver leur confidentialité tout en travaillant sur la plateforme.

b) Définition des contrats :

Voici les étapes générales pour définir les contrats sur Corda :

- **Définition des exigences :** il faut définir les exigences du contrat, telles que les conditions de participation, les obligations des participants, etc.

- **Codage du contrat :** le contrat doit être codé en utilisant le langage de programmation Kotlin. Corda fournit des bibliothèques et des modèles pour aider à coder les contrats.

- **Vérification du contrat :** il faut vérifier que le contrat est correctement codé et qu'il répond aux exigences définies.

- **Déploiement du contrat :** une fois le contrat codé et vérifié, il peut être déployé sur le réseau Corda pour être utilisé par les participants.

- **Mise à jour du contrat :** les contrats peuvent être mis à jour pour s'adapter aux nouveaux besoins du réseau.

En général, Corda utilise des contrats intelligents pour définir les règles qui régissent les transactions sur le réseau. Les contrats sont exécutés par les nodes du réseau pour garantir que les transactions respectent les conditions définies dans le contrat. Il est important de noter que les contrats doivent être correctement conçus et codés pour garantir une fonctionnalité fiable et une sécurité optimale.

c) Mise en place du réseau :

Voici les étapes générales pour mettre en place un réseau Corda :

- **Préparation du matériel :** il faut un ordinateur dédié pour créer le nœud Corda et une connexion internet stable.

- **Installation de Corda :** il faut télécharger et installer Corda sur le système.

- **Configuration du nœud :** le nœud Corda doit être configuré en spécifiant les paramètres tels que le nom d'hôte, le port et les clés publiques.

- **Mise en place de la base de données :** le nœud Corda utilise une base de données pour stocker les transactions et les contrats. Il faut donc mettre en place une base de données compatible avec Corda.

- **Mise en réseau des nodes :** les nodes Corda peuvent être mis en réseau en utilisant les adresses IP et les ports configurés.

- **Mise en place de la sécurité :** il est important de mettre en place une stratégie de sécurité pour protéger les données et les transactions sur le réseau.

- **Test et déploiement :** après avoir terminé les étapes ci-dessus, le réseau Corda peut-être tester en exécutant des transactions de test et en surveillant les performances. Une fois que tout est en ordre, le réseau peut être déployé pour une utilisation en production.

Il est important de noter que la mise en place d'un réseau Corda nécessite une connaissance approfondie de la technologie blockchain et des bonnes pratiques de sécurité. Il peut être nécessaire de recourir à un expert en la matière pour une mise en place réussie.

d) Création et envoi de transactions :

Voici les étapes générales pour créer et envoyer une transaction sur Corda :

- **Préparation des données :** les données nécessaires pour la transaction, telles que les informations sur les parties impliquées, les conditions de la transaction, etc., doivent être collectées et préparées.

- **Création de la transaction :** une fois les données préparées, la transaction peut être créée en utilisant le code Kotlin. Corda fournit des modèles pour aider à coder la transaction.

- **Vérification de la transaction :** il faut vérifier que la transaction est correctement codée et qu'elle répond aux exigences du contrat associé.

- **Envoi de la transaction :** une fois la transaction vérifiée, elle peut être envoyée à d'autres nodes sur le réseau Corda pour validation.
- **Validation de la transaction :** les nodes sur le réseau Corda valident la transaction en exécutant le contrat associé et en vérifiant que les conditions de la transaction sont remplies.

- **Enregistrement de la transaction :** une fois la transaction validée, elle est enregistrée sur la base de données distribuée du réseau Corda.

En général, les transactions sur Corda représentent des actions ou des événements sur le réseau. Les transactions sont soumises à des vérifications rigoureuses avant d'être enregistrées sur le réseau pour garantir la sécurité et la transparence des transactions. Il est important de noter que les transactions doivent être correctement conçues et codées pour garantir une fonctionnalité fiable et une sécurité optimale.

e) Validation des transactions :

La validation des transactions sur Corda implique l'exécution des contrats associés à la transaction pour vérifier que les conditions définies dans le contrat sont remplies. Voici les étapes générales de la validation des transactions sur Corda :

- **Réception de la transaction :** une fois une transaction envoyée sur le réseau Corda, les nodes la reçoivent et préparent la validation.

- **Exécution du contrat :** le contrat associé à la transaction est exécuté par les nodes sur le réseau Corda pour vérifier que les conditions de la transaction sont remplies.

- **Vérification des données :** les données associées à la transaction sont vérifiées pour s'assurer qu'elles sont correctes et valides.

- **Approbation ou rejet :** si les conditions du contrat sont remplies et que les données associées à la transaction sont correctes, la transaction est approuvée. Sinon, elle est rejetée.

- **Mise à jour de la base de données :** une fois la transaction approuvée, elle est enregistrée sur la base de données distribuée du réseau Corda.

En général, la validation des transactions sur Corda est un processus décentralisé qui implique plusieurs nodes sur le réseau. Cette approche garantit la transparence et la sécurité des transactions sur le réseau. Les contrats intelligents sont utilisés pour définir les règles qui régissent les transactions et garantir que les transactions respectent les conditions définies dans le contrat.

f) Stockage des données :

Le stockage de données sur Corda ne nécessite pas de matériel spécifique en dehors de l'infrastructure informatique standard pour exécuter les nœuds Corda. Les données sont stockées sur les disques durs des ordinateurs des nœuds Corda, et peuvent être stockées en utilisant une variété de systèmes de stockage de données, tels que des bases de données relationnelles ou NoSQL.

Cependant, pour des raisons de sécurité et de confidentialité, il est souvent recommandé d'utiliser des solutions de stockage sécurisées, telles que des disques durs cryptés ou des solutions de stockage de données en nuage chiffré. De plus, il peut être nécessaire d'utiliser des dispositifs de sauvegarde pour assurer la disponibilité des données à long terme.

En général, le choix des matériels de stockage dépend des exigences en matière de performance, de coût, de sécurité et de fiabilité de l'application Corda en question.

g) Mise à jour des contrats :

Pour mettre à jour un contrat sur Corda, vous pouvez suivre les étapes suivantes :

- Écrivez une nouvelle version du contrat en utilisant le même code de contrat existant.
- Téléchargez la nouvelle version sur les nœuds qui exécutent l'ancienne version.
- Mettez à jour la base de données pour refléter les modifications apportées au contrat.
- Exécutez les tests pour vous assurer que le nouveau contrat fonctionne correctement.
- Déployez le nouveau contrat sur la chaîne de production.

Il est important de faire ces mises à jour de manière coordonnée pour éviter les erreurs et les incohérences dans le réseau. Assurez-vous également de tester en profondeur le nouveau contrat avant de le déployer sur la chaîne de production pour éviter les problèmes potentiels.

7. ARGUMENTONS DANS LE RAPPORT SI LA TECHNOLOGIE EN QUESTION EST ADAPTEE POUR NOTRE BESOIN