ECOLE SUPERIEURE POLYTECHNIQUE DE DAKAR

DEPARTEMENT DE GENIE
INFORMATIQUE

THEME

Apport et Implications de la blockchain dans la gouvernance foncière.

Réalisé Par :

- Pape Ibra Ndiaye GLSI
- Zeinab abibatou Diallo GLSI
- Mame awa gueye SRT
- Boubacar bakery camara GLSI
- Cheikh ahmeth tidiane ndaw SRT

Encadré Par :

- Mr Mendy

PLAN

INTRODUCTION

I - Activités Préliminaires

I – 1 Etude du sujet

I– 2. Etude d'un système blockchain de consortium : cas d'Hyperledger Fabric (HLF)

I – 3. Etude des concepts de signature multiple

I-3.1 Signature multiple d'un document

I-3-2 Signature multiple de transaction : cas des wallets multisig

II - Multi signature de document et validation par smart contrat : Cas de **HLF**

CONCLUSION

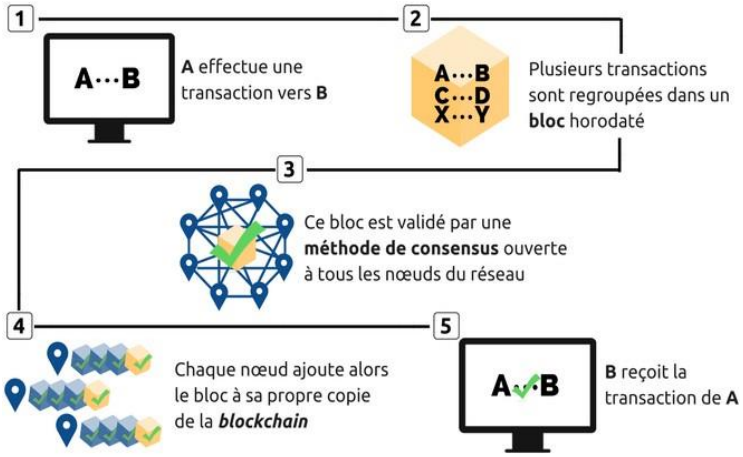
Introduction

La technologie Blockchain est un mécanisme de base de données avancé qui permet un partage transparent des informations au sein d'un réseau d'entreprises. Une base de données Blockchain stocke les données dans des blocs qui sont reliés entre eux dans une chaîne. Les données sont chronologiquement cohérentes, car vous ne pouvez pas supprimer ou modifier la chaîne sans le consensus du réseau. Par conséquent, vous pouvez utiliser la technologie Blockchain pour créer un grand livre inaltérable ou immuable pour le suivi des ordres, des paiements, des comptes et d'autres transactions. Le système dispose de mécanismes intégrés qui empêchent les entrées de transactions non autorisées et créent une cohérence dans la vue partagée de ces transactions.

Une blockchain est un registre, une grande base de données qui a la particularité d'être **partagée simultanément avec tous ses utilisateurs**, tous également détenteurs de ce registre, et qui ont également tous la capacité d'y inscrire des données, selon des règles spécifiques fixées par un protocole informatique très bien **sécurisé grâce à la cryptographie**.

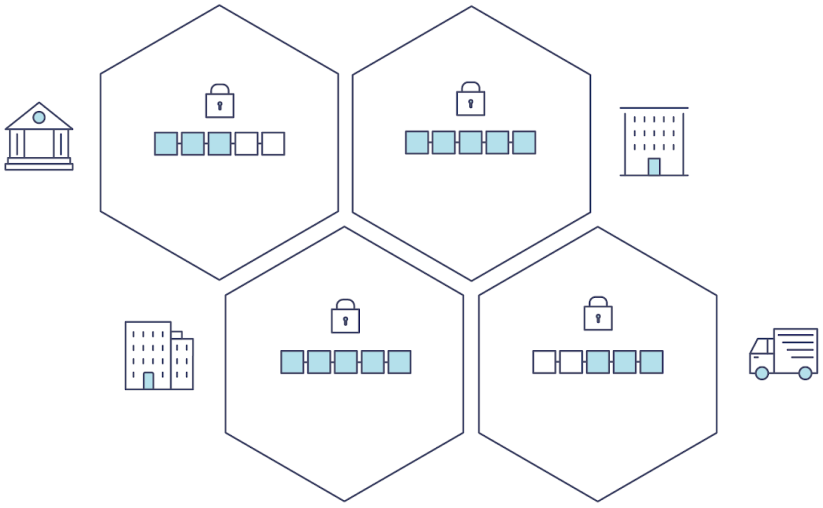
L'une des particularités de ce registre est d'enregistrer les données sur des **blocs** qui contiennent une quantité limitée d'informations. Un bloc validé ne peut plus être modifié, sauf par consensus des détenteurs du registre.

EXEMPLE D'ENREGISTREMENT D'UNE TRANSACTION



Source : Office parlementaire des choix scientifiques et technologiques

Au cœur d'un réseau blockchain se trouve un registre distribué qui enregistre toutes les transactions qui ont lieu sur le réseau.
Un registre blockchain est souvent décrit comme décentralisé car il est répliqué sur de nombreux participants au réseau, chacun d'entre eux collaborant à sa maintenance. Nous verrons que la décentralisation et la collaboration sont des attributs puissants qui reflètent la façon dont les entreprises échangent des biens et des services dans le monde réel.

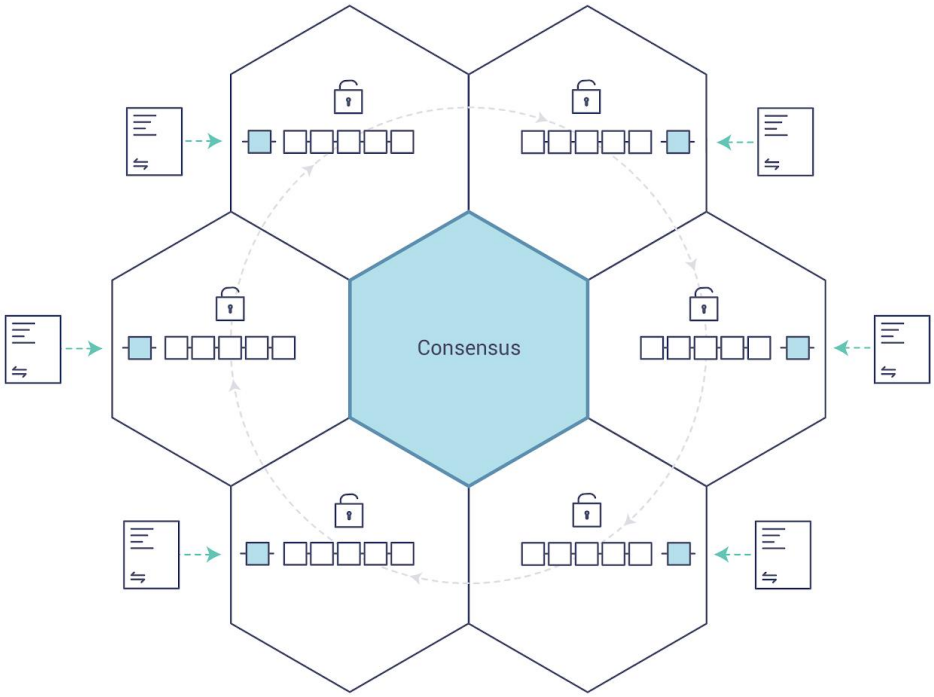


En plus d'être décentralisées et collaboratives, les informations enregistrées dans une blockchain sont en ajout uniquement, en utilisant des techniques cryptographiques qui garantissent qu'une fois qu'une transaction a été ajoutée au

registre, elle ne peut pas être modifiée. Cette propriété d'« immuabilité » permet de déterminer facilement la provenance des informations, car les participants peuvent être sûrs que les informations n'ont pas été modifiées après coup. C'est pourquoi les blockchains sont parfois décrites comme des systèmes de preuve.

Consensus

Le processus de synchronisation des transactions du grand livre sur le réseau - pour garantir que les grands livres ne sont mis à jour que lorsque les transactions sont approuvées par les participants appropriés, et que lorsque les grands livres sont mis à jour, ils sont mis à jour avec les mêmes transactions dans le même ordre - est appelé consensus.



Vous en apprendrez beaucoup plus sur les grands livres, les contrats intelligents et le consensus plus tard. Pour l'instant, il suffit de considérer une blockchain comme un système de transaction partagé et répliqué qui est mis à jour via des contrats intelligents et maintenu constamment synchronisé via un processus collaboratif appelé consensus.

Contrats intelligents

Pour prendre en charge la mise à jour cohérente des informations - et pour activer toute une série de fonctions de grand livre (transaction, interrogation, etc.) - un

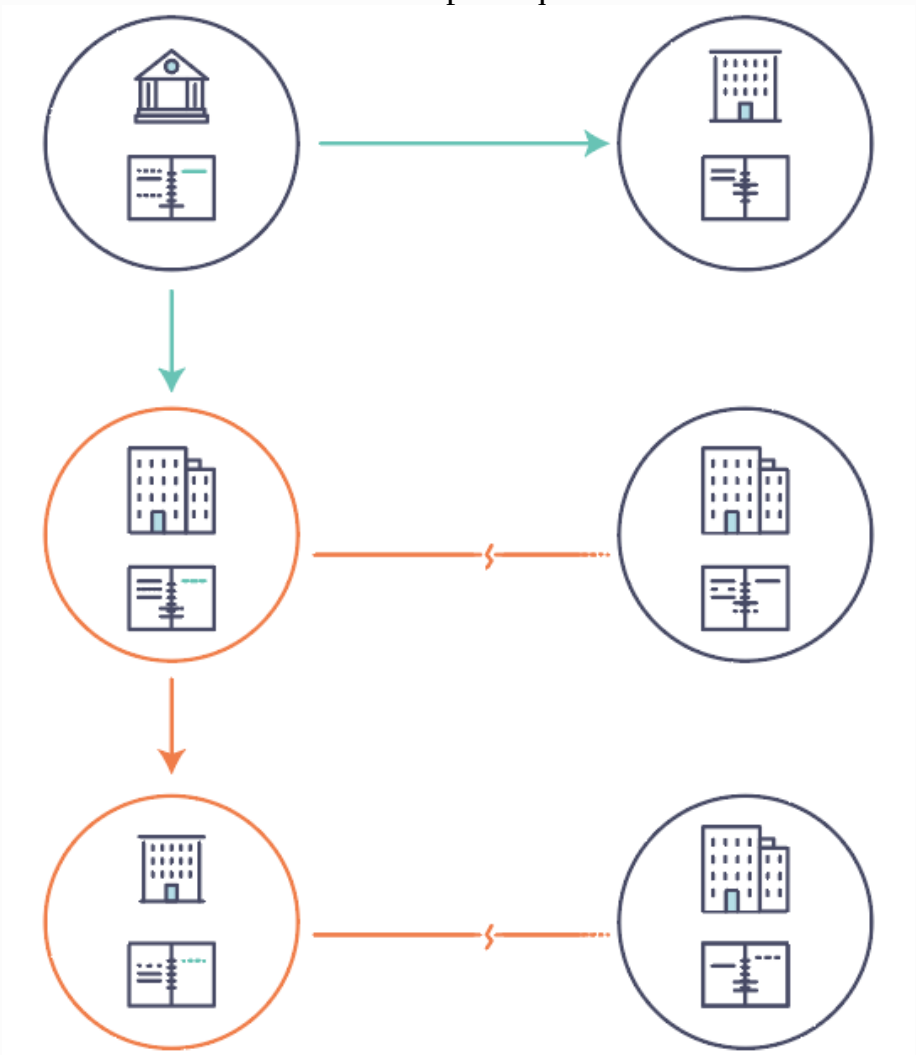
réseau blockchain utilise des contrats intelligents pour fournir un accès contrôlé au grand livre.

Les contrats intelligents ne sont pas seulement un mécanisme clé pour encapsuler les informations et les garder simples sur le réseau, ils peuvent également être écrits pour permettre aux participants d'exécuter automatiquement certains aspects des transactions.
Un contrat intelligent peut, par exemple, être écrit pour stipuler le coût d'expédition d'un article où les frais d'expédition changent en fonction de la rapidité avec laquelle l'article arrive. Avec les conditions convenues par les deux parties et écrites dans le grand livre, les fonds appropriés changent automatiquement de mains lorsque l'article est reçu.

Pourquoi une Blockchain est-elle utile ?

Les systèmes d'enregistrement d'aujourd'hui :

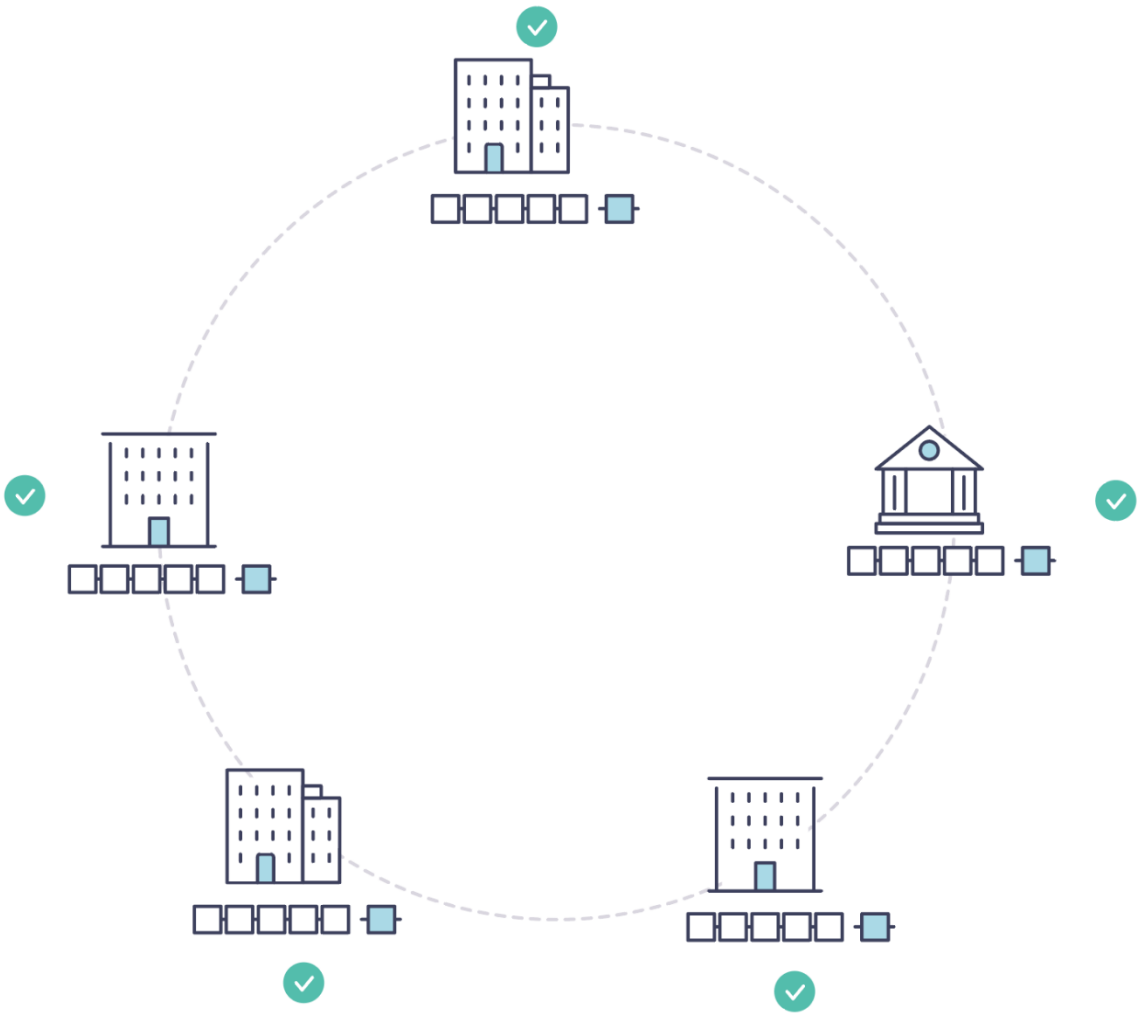
Les réseaux transactionnels d'aujourd'hui ne sont guère plus que des versions légèrement mises à jour des réseaux qui existent depuis que les dossiers commerciaux sont conservés. Les membres d'un réseau commercial effectuent des transactions entre eux, mais ils conservent des enregistrements distincts de leurs transactions. Et les choses qu'ils négocient - qu'il s'agisse de tapisseries flamandes au XVIe siècle ou de valeurs mobilières d'aujourd'hui - doivent avoir leur provenance établie chaque fois qu'elles sont vendues pour s'assurer que l'entreprise vendant un article possède une chaîne de titre vérifiant leur propriété.
Il vous reste un réseau d'entreprise qui ressemble à ceci :



La technologie moderne a fait passer ce processus des tablettes en pierre et des dossiers papier aux disques durs et aux plates-formes cloud, mais la structure sous-jacente est la même. Les systèmes unifiés de gestion de l'identité des participants au réseau n'existent pas, l'établissement de la provenance est si laborieux qu'il faut des jours pour régler les transactions sur titres (dont le volume mondial se compte en

plusieurs billions de dollars), les contrats doivent être signés et exécutés manuellement, et chaque base de données du système contient des informations uniques et représente donc un point de défaillance unique.
Avec l'approche fracturée actuelle du partage d'informations et de processus, il est impossible de créer un système d'enregistrement couvrant un réseau d'entreprise, même si les besoins de visibilité et de confiance sont clairs.

La différence blockchain
Et si, au lieu du nid de rats d'inefficacités représenté par le système « moderne » de transactions, les réseaux d'entreprise disposaient de méthodes standard pour établir l'identité sur le réseau, exécuter les transactions et stocker les données ? Et si l'établissement de la provenance d'un actif pourrait être déterminé en examinant une liste de transactions qui, une fois écrites, ne peuvent pas être modifiées, et donc fiables ?
Ce réseau d'entreprise ressemblerait plus à ceci :



Il s'agit d'un réseau blockchain, dans lequel chaque participant a sa propre copie répliquée du grand livre. Outre le partage des informations du grand livre, les processus de mise à jour du grand livre sont également partagés. Contrairement aux systèmes actuels, où les programmes privés d'un participant sont utilisés pour mettre à jour leurs registres privés , un système de blockchain a des programmes partagés pour mettre à jour les registres partagés .
Avec la possibilité de coordonner leur réseau d'entreprise via un registre partagé, les réseaux de blockchain peuvent réduire le temps, les coûts et les risques associés aux informations privées et au traitement tout en améliorant la confiance et la visibilité.
Vous savez maintenant ce qu'est la blockchain et pourquoi elle est utile. Il y a beaucoup d'autres détails qui sont importants, mais ils sont tous liés à ces idées fondamentales de partage d'informations et de processus.

I - Activités Préliminaires

I – 1 Etude du sujet

Après avoir parcouru l’article de Aanchal Anand, Matthew McKibbin, et Frank Pichel, nous avons trouvé certaines ressources portant sur l’apport et l’implication de la blockchain dans la gouvernance foncière.

En effet, le concept d'un registre public transparent et décentralisé pourrait facilement s'appliquer à la gestion de l'information foncière, où le registre foncier sert de base de données de tous les droits de propriété et transactions historiques. L'avantage supplémentaire de l'utilisation de la technologie blockchain est que l'on peut s'éloigner d'une base de données centralisée, qui trop souvent pourrait être vulnérable au piratage, à une mauvaise utilisation par les administrateurs système ou même à des catastrophes naturelles ou causées par l'homme détruisant le centre de données.

Lors de l'examen des applications potentielles de la technologie blockchain, certaines utilisations potentielles passent au premier plan, telles que :

- l'horodatage des transactions semblable à la notarisation virtuelle
- reprise après sinistre car le système ne repose pas sur un seul centre de données

- enregistrement des détails dans un environnement inviolable et immuable
- utiliser des "pièces colorées" pour gérer les détails du registre. Chacune de ces applications potentielles sera développée plus loin dans cet article.

D'autre part, afin d'analyser comment la blockchain pourrait être mise en œuvre pour prendre en charge les transactions dans le SIL, il est nécessaire de comprendre les processus cadastraux et les transactions dans le LIS, ainsi que les aspects législatifs et organisationnels du LIS. Le système d'information cadastrale est maintenu par l'autorité géodésique centrale. La loi sur l'arpentage et le cadastre en Serbie définit le système d'information géodésique-cadastral comme un système qui contient des données et des services pour les travaux géodésiques de base, le cadastre immobilier, le registre d'adresses, le cadastre des services publics, etc. Son objectif est de permettre la gestion, la maintenance, l'accès et l'utilisation des données cadastrales (à la fois alphanumériques et géospatiales).

Les utilisateurs peuvent se connecter aux services d'administration en ligne à l'aide de leurs certificats numériques qualifiés, de documents numériques qui lient la clé publique de l'utilisateur à l'identité de l'utilisateur et à l'autorité de certification qui a vérifié le contenu du certificat. Ces certificats numériques qualifiés permettent aux utilisateurs de se connecter en toute sécurité au système et de prouver leur identité sont fournis au niveau national en Serbie. Les blockchains autorisées exigent que l'identité d'un utilisateur soit vérifiée avant qu'il ne puisse accéder ou utiliser la blockchain. Par conséquent, pour créer un compte sur un réseau blockchain public autorisé, un lien vers une identité réelle doit être créé. Chaque utilisateur doit créer son propre compte et se connecter avec le certificat numérique. De même, les personnes morales peuvent également posséder leurs certificats numériques.

I– 2. Etude d'un système blockchain de consortium : cas d'Hyperledger Fabric (HLF)

- **Documentation sur Hyperledger Fabric** :

La Fondation Linux a fondé le projet Hyperledger en 2015 pour faire progresser les technologies de blockchain intersectorielles. Plutôt que de déclarer une seule norme de blockchain, il encourage une approche collaborative pour développer des technologies de blockchain via un processus communautaire, avec des droits de

propriété intellectuelle qui encouragent le développement ouvert et l'adoption de normes clés au fil du temps.

Hyperledger Fabric est l'un des projets de blockchain au sein d'Hyperledger. Comme d'autres technologies de blockchain, il a un grand livre, utilise des contrats intelligents et est un système par lequel les participants gèrent leurs transactions. Là où Hyperledger Fabric se démarque de certains autres systèmes de blockchain, c'est qu'il est privé et autorisé. Plutôt qu'un système ouvert sans autorisation qui permet à des identités inconnues de participer au réseau (nécessitant des protocoles tels que la "preuve de travail" pour valider les transactions et sécuriser le réseau), les membres d'un réseau Hyperledger Fabric s'inscrivent via un fournisseur de services d'adhésion (MSP) de confiance.

Hyperledger Fabric propose également plusieurs options enfichables. Les données du grand livre peuvent être stockées dans plusieurs formats, les mécanismes de consensus peuvent être échangés et différents MSP sont pris en charge.

Hyperledger Fabric offre également la possibilité de créer des canaux, permettant à un groupe de participants de créer un registre de transactions distinct. Il s'agit d'une option particulièrement importante pour les réseaux où certains participants peuvent être des concurrents et ne veulent pas que chaque transaction qu'ils effectuent - un prix spécial qu'ils offrent à certains participants et pas à d'autres, par exemple - soit connue de chaque participant. Si deux participants forment un canal, alors ces participants - et aucun autre - ont des copies du grand livre pour ce canal.

Registre partagé

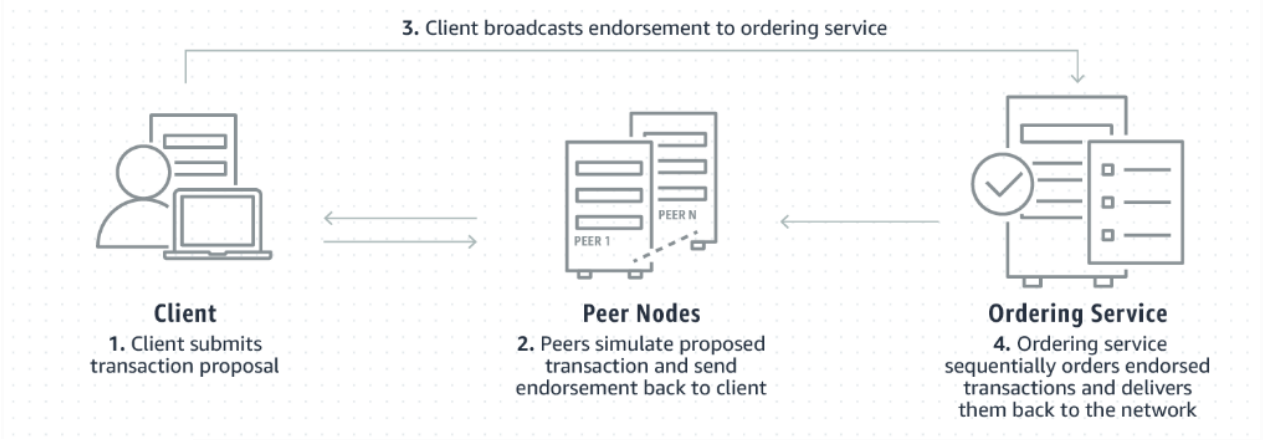
Hyperledger Fabric possède un sous-système de registre comprenant deux composants : l'état mondial et le journal des transactions. Chaque participant dispose d'une copie du registre de chaque réseau Hyperledger Fabric auquel il appartient.

Le composant d'état mondial décrit l'état du grand livre à un moment donné. C'est la base de données du grand livre. Le composant de journal des transactions enregistre toutes les transactions qui ont abouti à la valeur actuelle de l'état mondial ; c'est l'historique des mises à jour pour l'état du monde. Le grand livre est donc une combinaison de la base de données d'état mondial et de l'historique du journal des transactions.

Le grand livre a un magasin de données remplaçable pour l'état du monde. Par défaut, il s'agit d'une base de données de stockage clé-valeur LevelDB. Le journal des transactions n'a pas besoin d'être enfichable. Il enregistre simplement les valeurs avant et après de la base de données du grand livre utilisée par le réseau blockchain.

Hyperledger Fabric est une plate-forme pour les solutions de registre distribué reposant sur une architecture modulaire offrant des degrés élevés de confidentialité, de résilience, de flexibilité et d'évolutivité. Il est conçu pour prendre en charge les

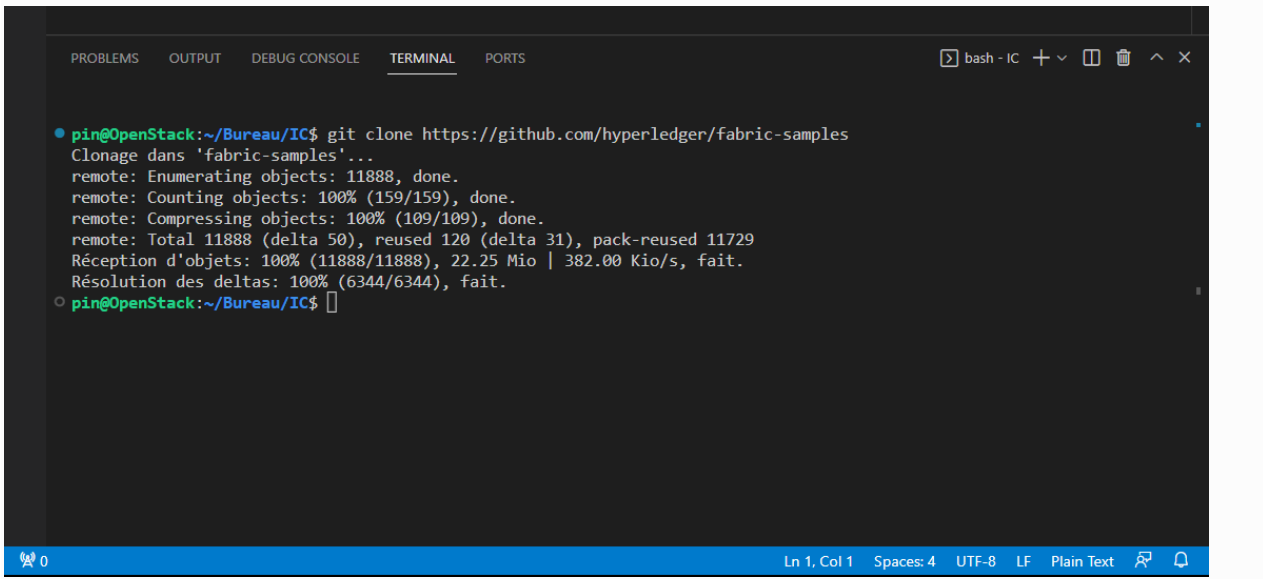
implémentations enfichables de différents composants et s'adapter à la complexité et aux subtilités qui existent dans l'écosystème économique.

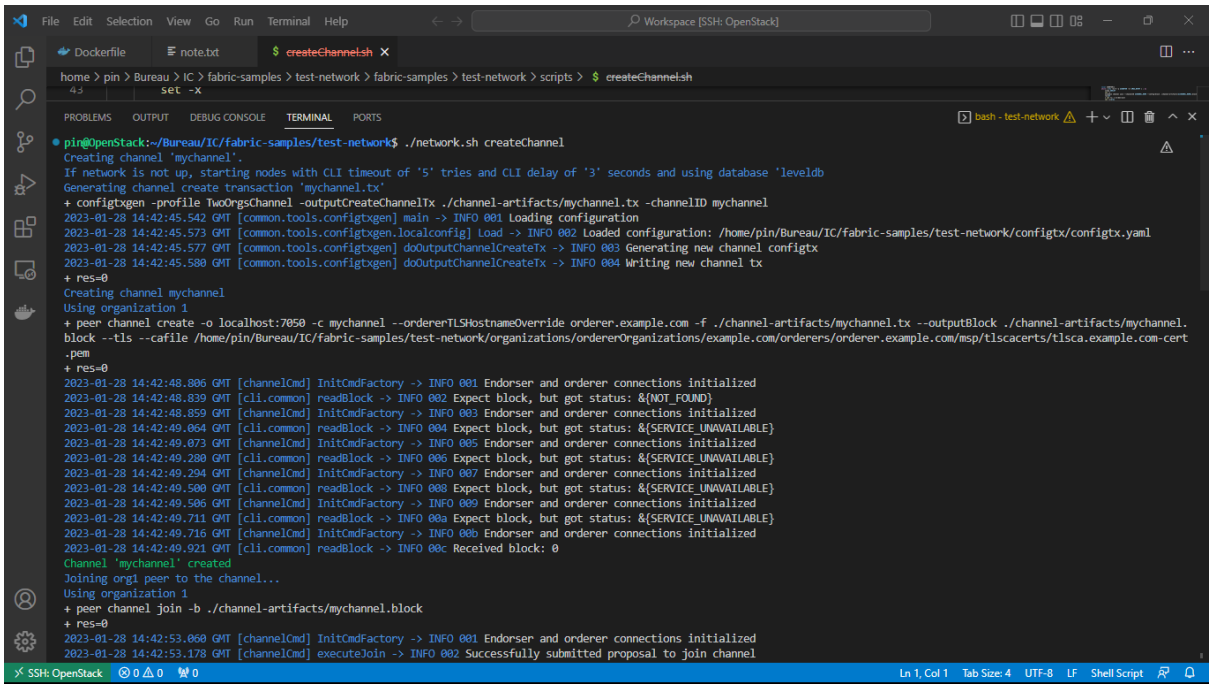


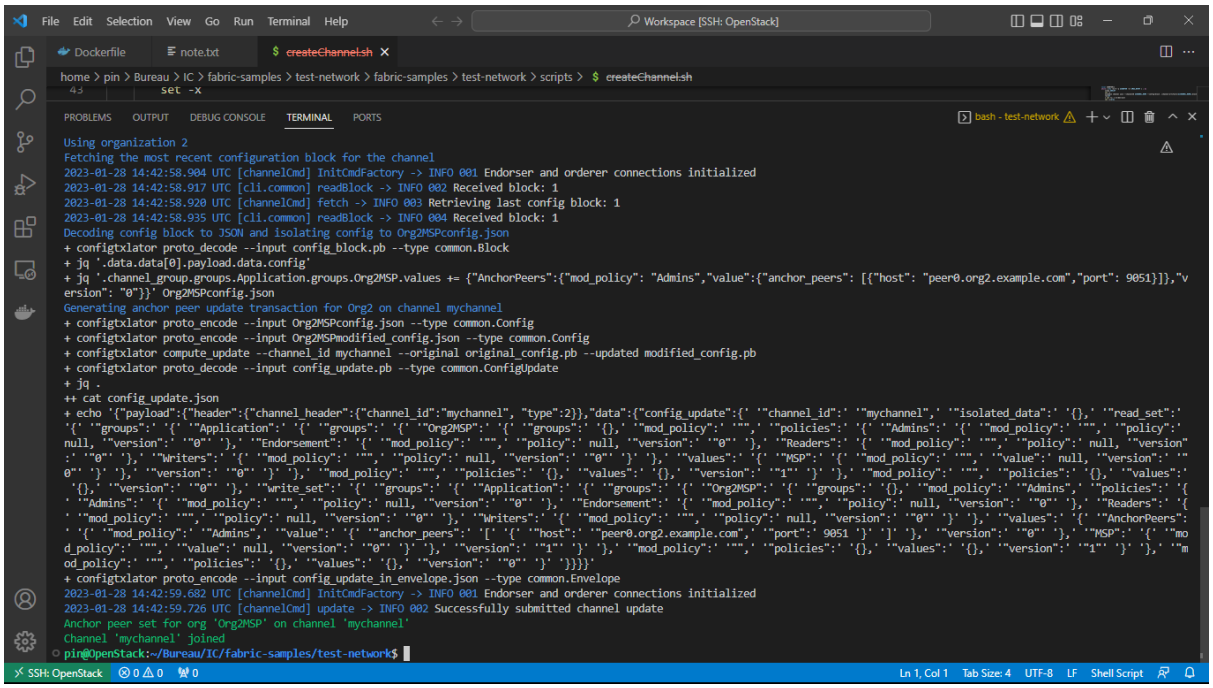
Flux de transaction HyperLedger Fabric

- **<u>Déployer un premier réseau HLF et exécuter une transaction</u> :**

Clonage du repository de fabric samples







- **<u>Argumenter dans le rapport si la technologie en question est adaptée pour notre besoin</u>** :

Pour augmenter dans le rapport si la technologie en question est adaptée à nos besoins, nous pouvons mettre en avant les points suivants:

1. **Contrôle de l'identité** : HLF permet un contrôle rigoureux des identités des membres du consortium, ce qui garantit que les participants autorisés peuvent accéder aux données et aux transactions.
2. **Confidentialité** : HLF utilise des techniques de confidentialité pour protéger les données sensibles, ce qui garantit que seuls les participants autorisés peuvent accéder à ces informations.
3. **Scalabilité** : HLF a été conçue pour être évolutive, ce qui signifie que le système peut être adapté pour répondre aux besoins croissants des membres du consortium.
4. **Interopérabilité** : HLF est conçu pour être interopérable avec d'autres systèmes et technologies, ce qui signifie que vous pouvez intégrer facilement HLF dans votre architecture existante.
5. **Modularité** : HLF est une plateforme modulaire qui vous permet de personnaliser et de configurer les fonctionnalités en fonction de vos besoins spécifiques.
6. **Durabilité** : HLF est une plateforme open-source qui a été développée par une grande communauté de développeurs, ce qui garantit la durabilité et la robustesse de la plateforme.

I – 3. Etude des concepts de signature multiple

I-3.1 Signature multiple d'un document

- Le principe de la multisignature est très simple: il permet de faire signer de façon numérique un seul document à un groupe d'utilisateurs.
- Pour autoriser une transaction sur le réseau avec la multi-signature, il faut plus d'une clé, alors que les transactions standards sont de type transactions à signature unique

I-3-2 Signature multiple de transaction : cas des wallets multisig

- Un wallet MultiSig utilise plusieurs clés privées pour autoriser les transactions cryptographiques.

- Ils peuvent également être configurés pour permettre à chacun dans l'ensemble de clés privées de générer une signature.
- La détention de clés privées à différents endroits améliore la sécurité, tandis que le fait de permettre à plusieurs clés de signer une transaction améliore la convivialité.

II - Multi signature de document et validation par smart contrat **: Cas de HLF**

Conclusion

En raison de ses fonctionnalités telles que le contrôle de l'identité, la confidentialité, la scalabilité, l'interopérabilité, la modularité et la durabilité, HLF est un choix solide pour les consortiums qui cherchent à développer des applications blockchain fiables et sécurisées pour répondre aux besoins de leur gestion foncière.