Université Cheikh Anta Diop de Dakar

Ecole Supérieure Polytechnique

ECOLE SUPERIEURE
POLYTECHNIQUE

Département Génie Informatique

A7 : Etude d'un système blockchain de consortium cas de Quorum

Groupe 7

Présenté par :

Anta Diop MBAYE

Mame Meissa DIENG

Victorine Sady NDIAYE

Zeinebou Mohamed MAHMOUD

Classe : M2GLSI

Année universitaire : 2022/2023

PLAN

I. Etude du sujet

I.1 Qu'est-ce que la Blockchain ?

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.

I.2 Blockchain dans l'administration des biens fonciers

Dans l'administration des biens fonciers la blockchain peut être utilisée pour :

- Stocker et gérer les enregistrements de propriété foncière de manière transparente, sécurisée et efficace ;
- Aider à éliminer les erreurs et les fraude dans les enregistrements fonciers ;
- Améliorer la transparence dans les transactions immobilières et faciliter la gestion des conflits liés à la propriété foncière ;
- Rendre le processus de transfert de propriété plus rapide et moins coûteux en automatisant de nombreuses étapes.

II. Présentation de Quorum

II.1 Définition de Quorum Blockchain

Quorum est à la base une plateforme de blockchain privée qui a été mise en place comme soft fork de l'Ethereum **par JP Morgan Chase** qui se trouve être une structure financière extrêmement développée dans le secteur. En gardant comme base les principales spécificités de l'ETH, le quorum a tout de même ajouté ses propres options à l'image de :

- La création de réseaux privés ;
- La confidentialité des échanges ;
- Un haut débit de transaction.

Ajoutons à cela que Quorum reste une création en open source, c'est-à-dire qu'il s'agit d'un programme web ouvert auquel peut contribuer n'importe quel autre développeur. Ayant comme base l'Ethereum, le Quorum présente le même langage de programmation à savoir Solidity qui est déjà connu par les nombreux utilisateurs de la crypto. Il en va de même pour les devises ou encore les jetons créés sur le projet qui seront compatibles avec les normes appliquées par l'ETH.

II.2 Comment fonctionne Quorum?

Le fonctionnement de Quorum se base sur des nœuds validateurs qui sont autorisés à valider les transactions et à maintenir une copie de la chaîne de blocs. Pour valider une transaction, un certain nombre de nœuds doivent atteindre un consensus sur son validité. Ce nombre est défini par le Quorum.

Quorum offre également une confidentialité accrue en permettant aux parties impliquées dans une transaction de contrôler qui peut voir les détails de la transaction. Les transactions confidentielles sont cryptées et accessibles uniquement aux participants autorisés.

II.3 Les avantages et les limites de Quorum Blockchain

Ce système a plusieurs avantages et caractéristiques :

- Sans intermédiaire : Les utilisateurs sont connectés les **uns aux autres** (système peer 2 peer, pair à pair).
- Conséquence directe du premier point, il n'y a **ni organe de contrôle ni tiers de confiance** (si ce n'est l'ensemble des utilisateurs), ce qui a de nombreux impacts et ouvre beaucoup de potentialités.
- **Sécurisée** et très difficilement piratable : Puisque chacun peut librement devenir un nœud du réseau, il deviendra lui-même hébergeur des données, ce qui ajoute à chaque fois un point de contrôle. Il faudrait pour pouvoir pirater le système posséder plus de la moitié des nœuds pour envoyer des informations erronées, ce qui devient très difficile dès qu'il y a plusieurs milliers d'utilisateurs du système.
- L'impossibilité d'effacer des données : C'est un autre avantage de la blockchain, toutes les informations stockées à chaque nouveau bloc ne peuvent plus être modifiées ou supprimées.

Les limites de Quorum incluent les éléments suivants :

- **Scalabilité :** Comme avec de nombreux autres systèmes de blockchain, Quorum peut avoir des problèmes de scalabilité lorsqu'il est soumis à une forte demande de transactions.
- **Complexité :** La mise en place et la gestion d'un réseau Quorum peuvent être complexes et nécessitent une expertise technique.
- **Confidentialité :** Bien que Quorum offre une confidentialité accrue par rapport à d'autres systèmes de blockchain publics, cela peut également présenter des défis en termes de protection de la vie privée et de conformité réglementaire.
- **Interopérabilité :** Quorum est conçu pour fonctionner en interne au sein d'une organisation, il peut donc être difficile d'interconnecter différents réseaux Quorum entre eux.
- **Coût :** L'utilisation de Quorum peut entraîner des coûts supplémentaires pour les infrastructures informatiques et les ressources humaines nécessaires pour le mettre en place et le gérer.

III. Implémentation

On commence par créer un répertoire sur notre VM :

```
root@meissadieng-VirtualBox:~# mkdir quorum
root@meissadieng-VirtualBox:~# cd quorum/
root@meissadieng-VirtualBox:~/quorum#
```

Puis on installe le **quorum-wizard**

```
root@meissadieng-VirtualBox:~/quorum# sudo npm install -g quorum-wizard
/usr/bin/quorum-wizard -> /usr/lib/node_modules/quorum-wizard/build/index.js
+ quorum-wizard@1.3.3
added 176 packages from 125 contributors in 43.292s
root@meissadieng-VirtualBox:~/quorum#
```

Une fois installé, on peut lancer la commande suivante :

```
root@meissadieng-VirtualBox:~/quorum# quorum-wizard
?
Welcome to Quorum Wizard!

This tool allows you to easily create bash, docker, and kubernetes files to sta
rt up a quorum network.
You can control consensus, privacy, network details and more for a customized s
etup.
Additionally you can choose to deploy our chain explorer, Cakeshop, to easily v
iew and monitor your network.

We have 3 options to help you start exploring Quorum:

  1.  Quickstart - our 1 click option to create a 3 node raft network with tess
era and cakeshop

  2.  Simple Network - using pregenerated keys from quorum 7nodes example,
      this option allows you to choose the number of nodes (7 max), consensus m
echanism, transaction manager, and the option to deploy cakeshop
```

L'installeur nous propose alors plusieurs choix, nous allons sélectionner **'Quickstart'** :

```
(Use arrow keys)
❯ Quickstart (3-node raft network with tessera and cakeshop)
  Simple Network
  Custom Network
  Generate from Existing Configuration
  Exit
```

Si tout s'est bien passé, vous devriez voir quelque le message **'Quorum network created'** comme ci-dessous :

```
Tessera Node 1 public key:
BULeR8JyUWhiuuCMU/HLA0Q5pzkYT+cHII3ZKBey3Bo=

Tessera Node 2 public key:
QfeDAys9MPDs2XHExtc84jKGHxZg/aj52DTh0vtA3Xc=

Tessera Node 3 public key:
1iTZde/ndBHvzhcl7V68x44Vx7pl8nwx9LqnM/AfJUg=

------------------------------------------------------------------------------
-


Quorum network created

Run the following commands to start your network:

cd /root/quorum/network/3-nodes-quickstart
./start.sh

A sample simpleStorage contract is provided to deploy to your network
To use run ./runscript.sh public_contract.js from the network folder

A private simpleStorage contract was created with privateFor set to use Node 2'
s public key: QfeDAys9MPDs2XHExtc84jKGHxZg/aj52DTh0vtA3Xc=
```

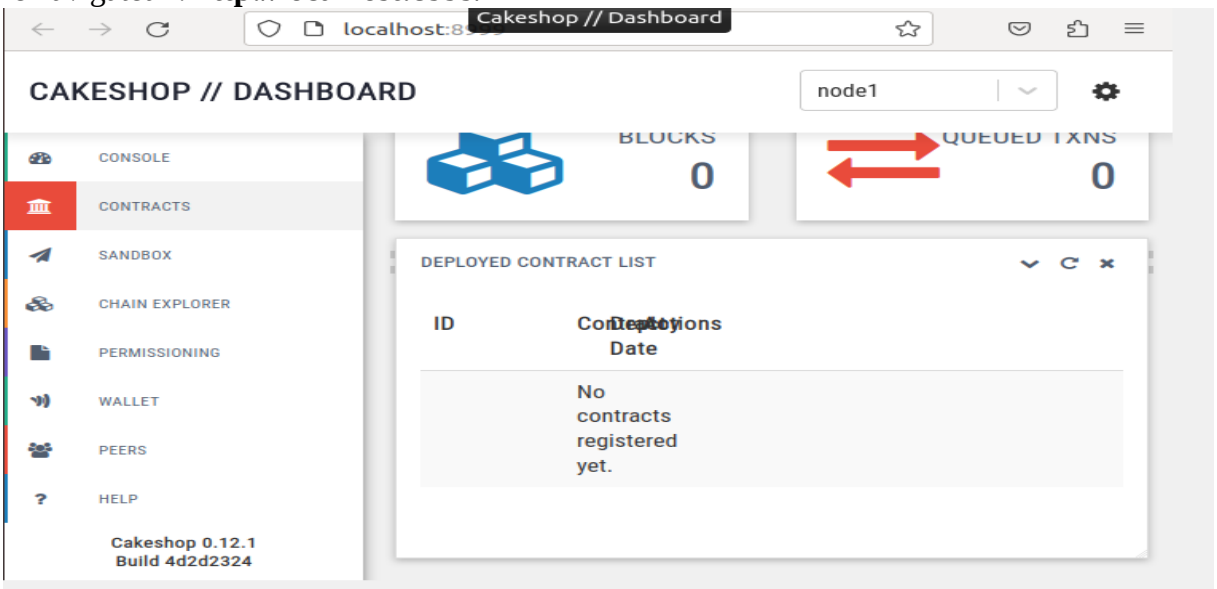
Maintenant que tout est prêt, on peut aller lancer notre blockchain

```
root@meissadieng-VirtualBox:~/quorum# cd network/3-nodes-quickstart/
root@meissadieng-VirtualBox:~/quorum/network/3-nodes-quickstart# ./start.sh
```

Lorsque le script se termine :

```
Cakeshop is not yet listening on http
Waiting until Cakeshop is running...
Cakeshop is not yet listening on http
Waiting until Cakeshop is running...
Cakeshop is not yet listening on http
Waiting until Cakeshop is running...
Cakeshop started at http://localhost:8999
Successfully started Quorum network.
--------------------------------------------------------------------------------
-

Tessera Node 1 public key:
BULeR8JyUWhiuuCMU/HLA0Q5pzkYT+cHII3ZKBey3Bo=

Tessera Node 2 public key:
QfeDAys9MPDs2XHExtc84jKGHxZg/aj52DTh0vtA3Xc=

Tessera Node 3 public key:
1iTZde/ndBHvzhcl7V68x44Vx7pl8nwx9LqnM/AfJUg=

--------------------------------------------------------------------------------
-

root@meissadieng-VirtualBox:~/quorum/network/3-nodes-quickstart#
```

Pour l'utiliser, si l'étape précédente s'est bien passée, il suffit d'ouvrir l'adresse suivante dans le navigateur : **http://localhost:8999/**

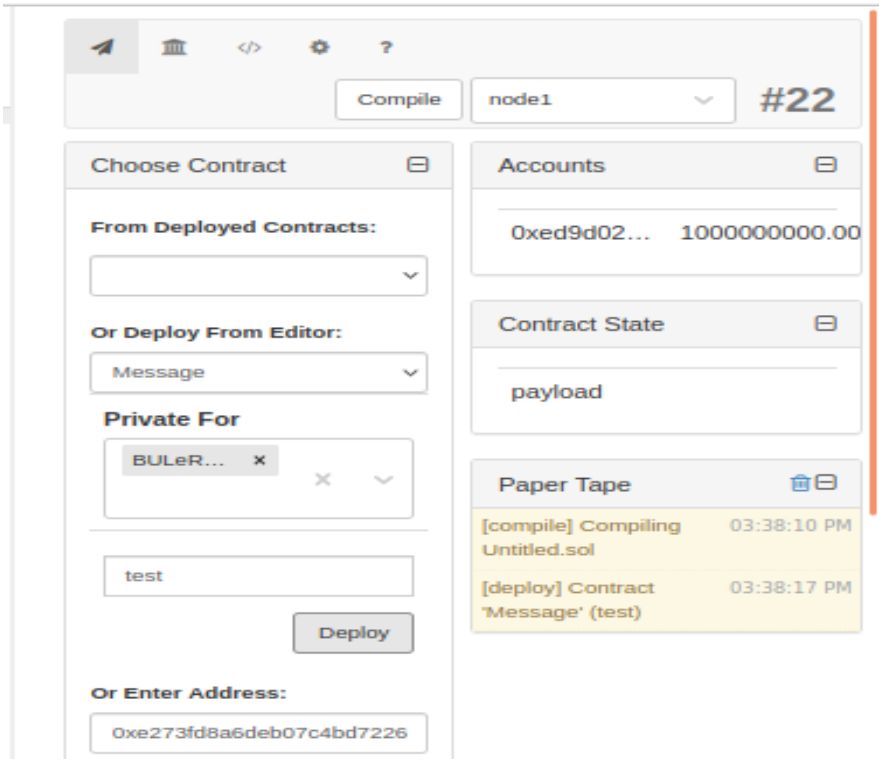


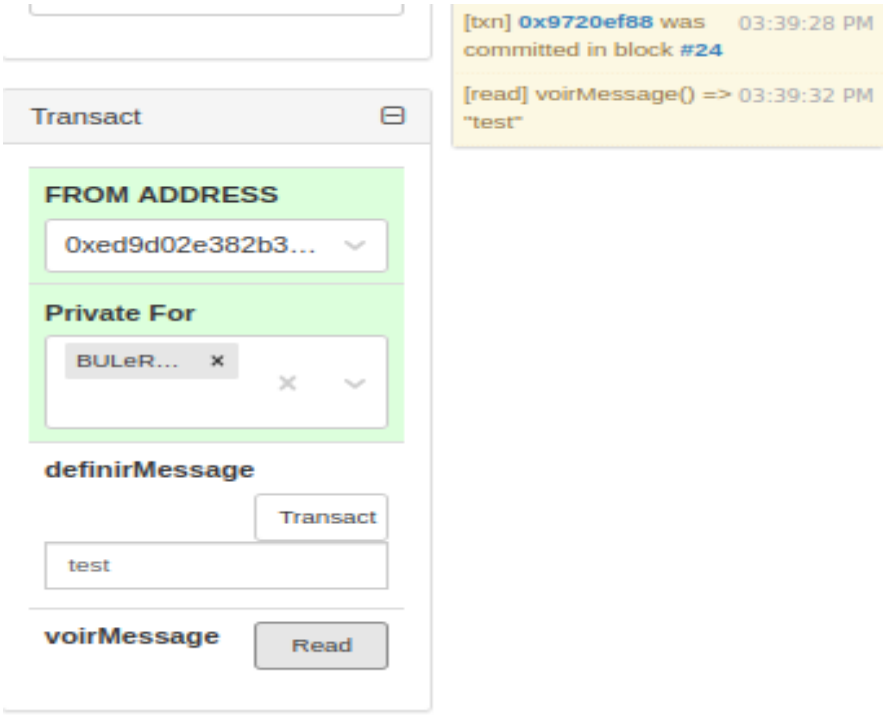
- **Déploiement d'un premier réseau et exécution d'une transaction**

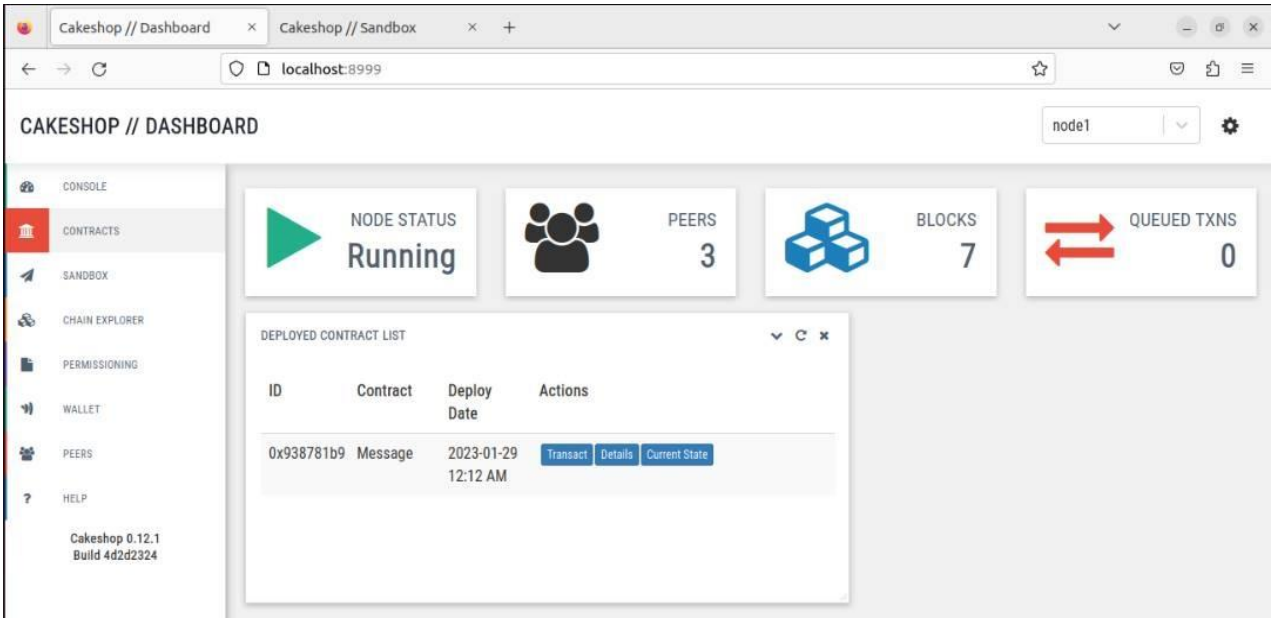
Nous allons maintenant déployer un premier réseau et exécuter une transaction

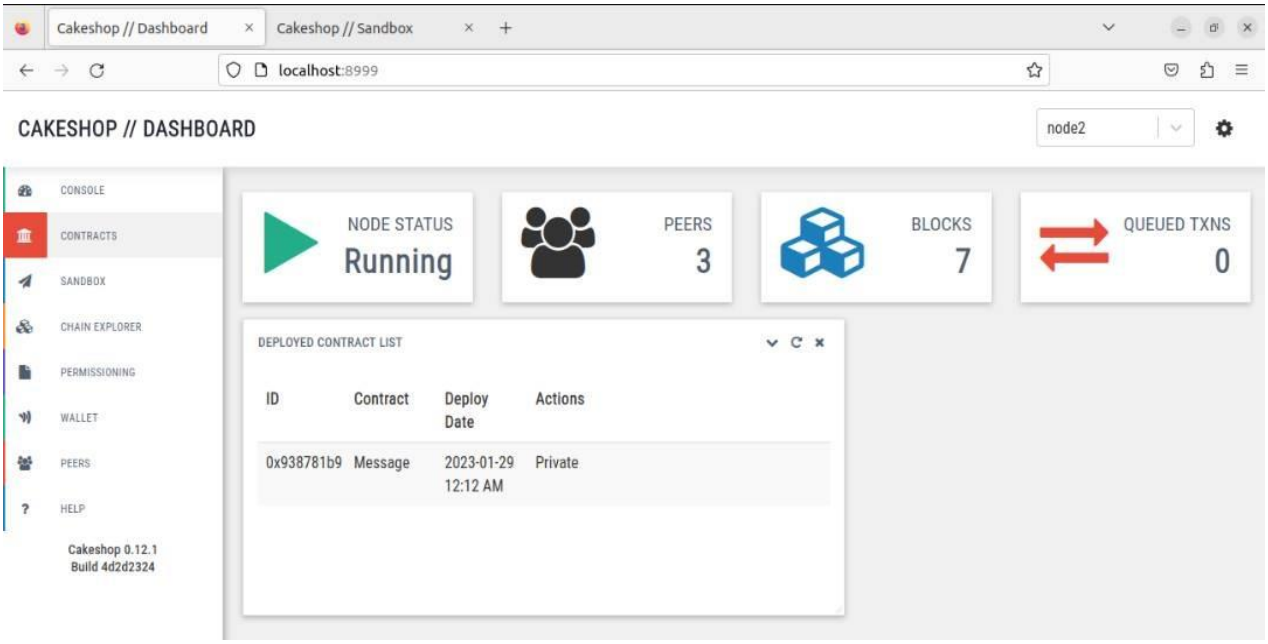
Voici le code du contrat :

```
pragma solidity >=0.4.22 <0.9.0;

contract Message {

    string lemessage;

    constructor(string memory _messageoriginal) public {
        lemessage = _messageoriginal;
    }

    function definirMessage(string memory _nouveaumessage) public{
        lemessage = _nouveaumessage;
    }

    function voirMessage() public view returns (string memory){
        return lemessage;
    }

}
```

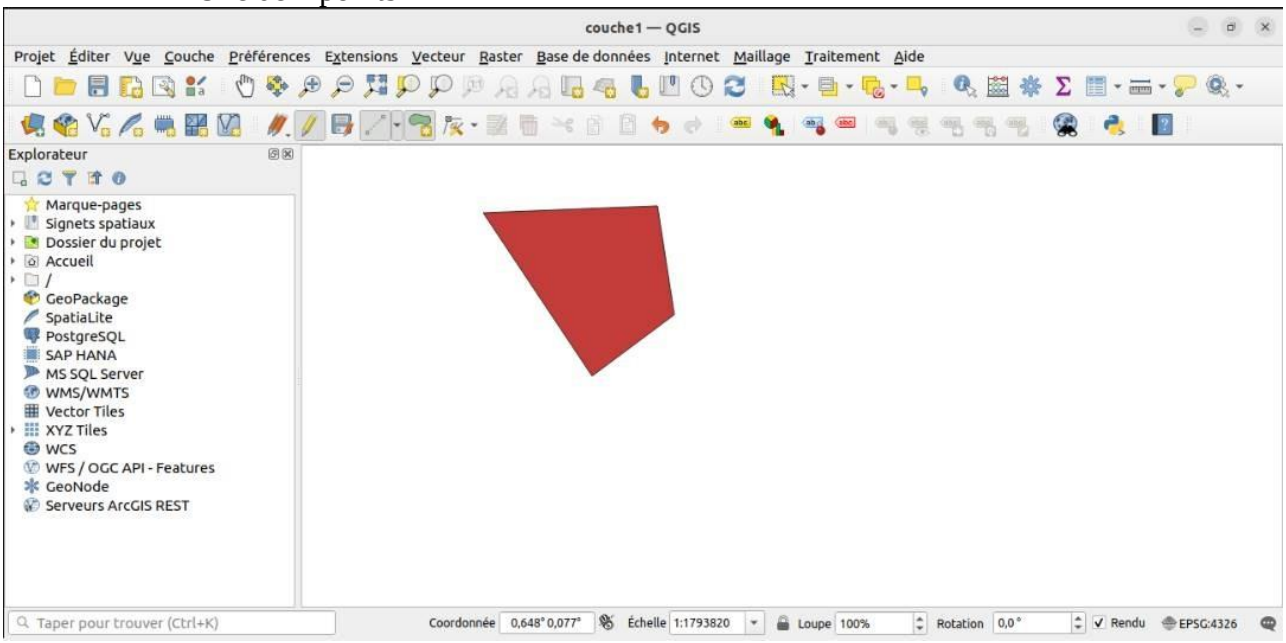



[txn] 0x9720ef88 was committed in block #24
03:39:28 PM
[read] voirMessage() => "test"
03:39:32 PM
Transact
FROM ADDRESS
0xed9d02e382b3...
Private For
BULeR...
definirMessage
Transact
test
voirMessage
Read

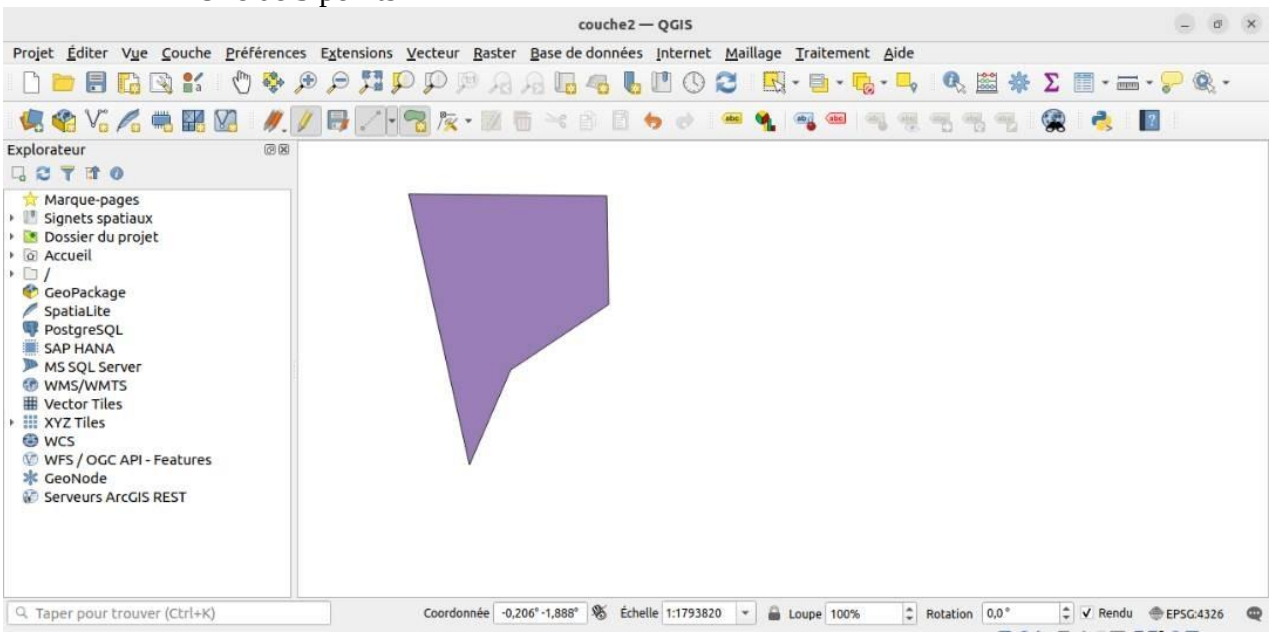

Cakeshop // Dashboard
Cakeshop // Sandbox
localhost:8999
CAKESHOP // DASHBOARD
node1
CONSOLE
CONTRACTS
SANDBOX
CHAIN EXPLORER
PERMISSIONING
WALLET
PEERS
HELP
Cakeshop 0.12.1
Build 4d2d2324
NODE STATUS
Running
PEERS
3
BLOCKS
7
QUEUED TXNS
0
DEPLOYED CONTRACT LIST
ID
Contract
Deploy Date
Actions
0x938781b9
Message
2023-01-29 12:12 AM
Transact
Details
Current State



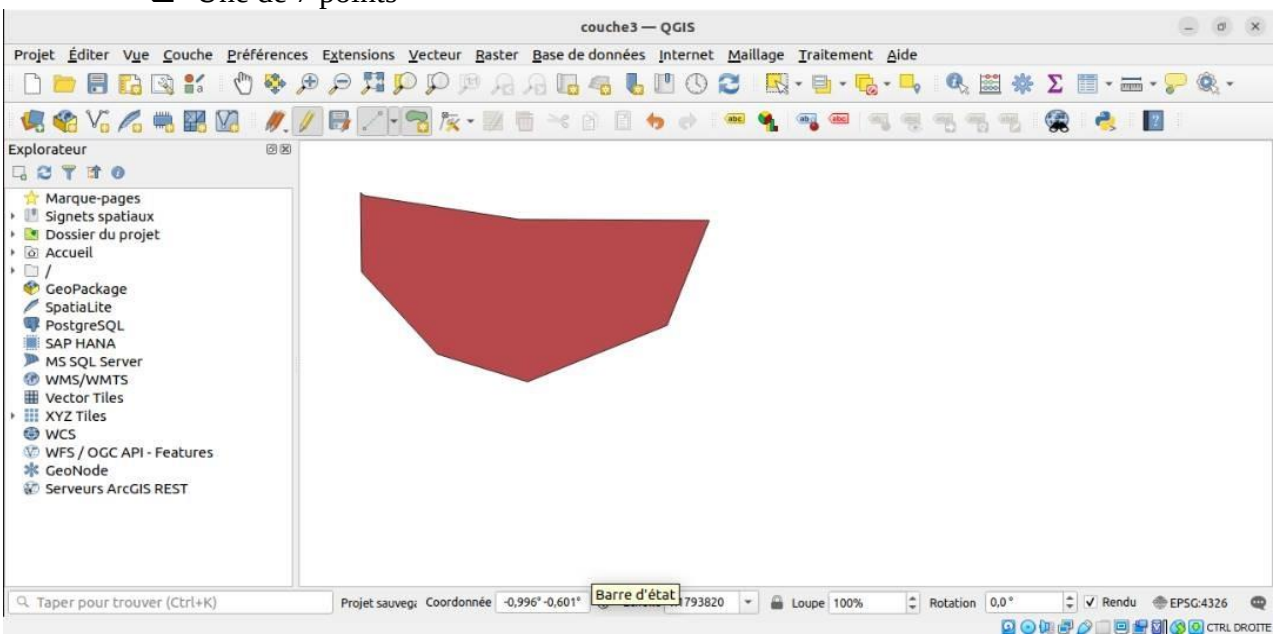
- **Création des parcelles avec QGIS**
  - ❑ Une de 4 points



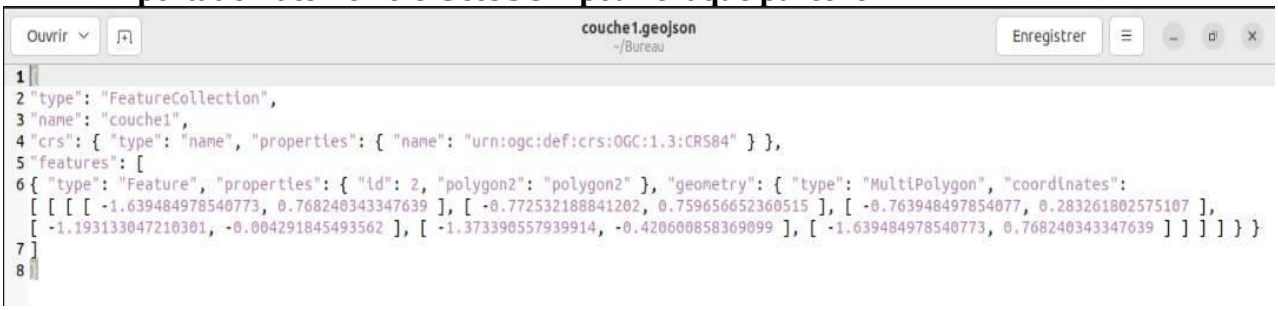
- ❑ Une de 5 points

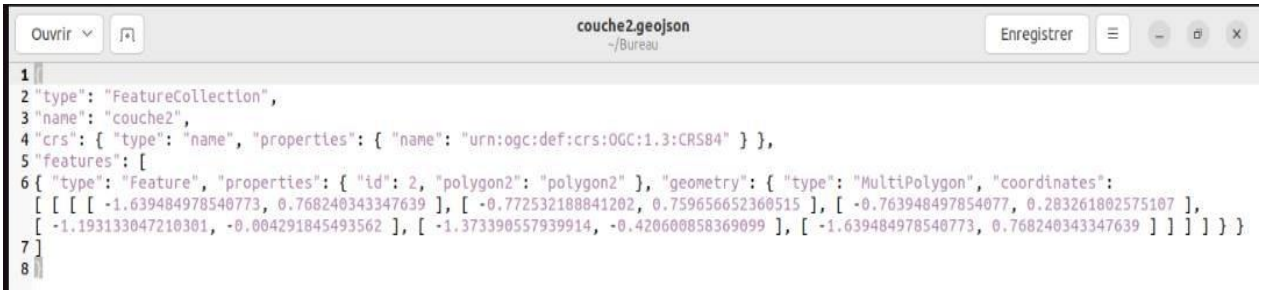


- ❑ Une de 7 points



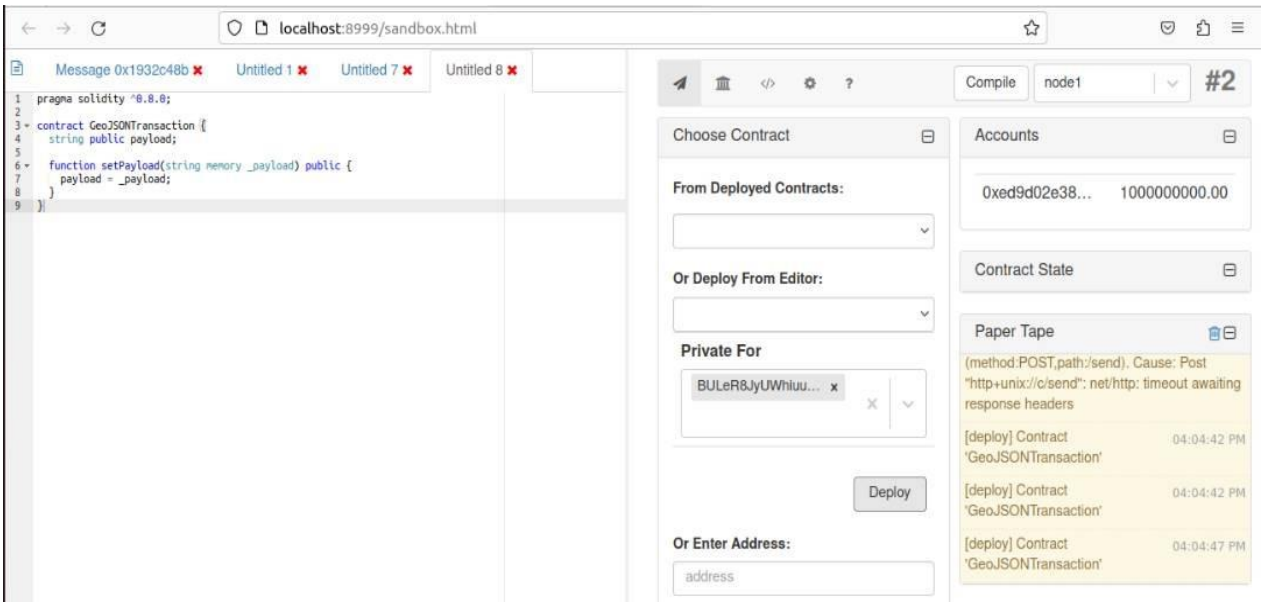
- **Exportation des fichiers GeoJSON pour chaque parcelle**



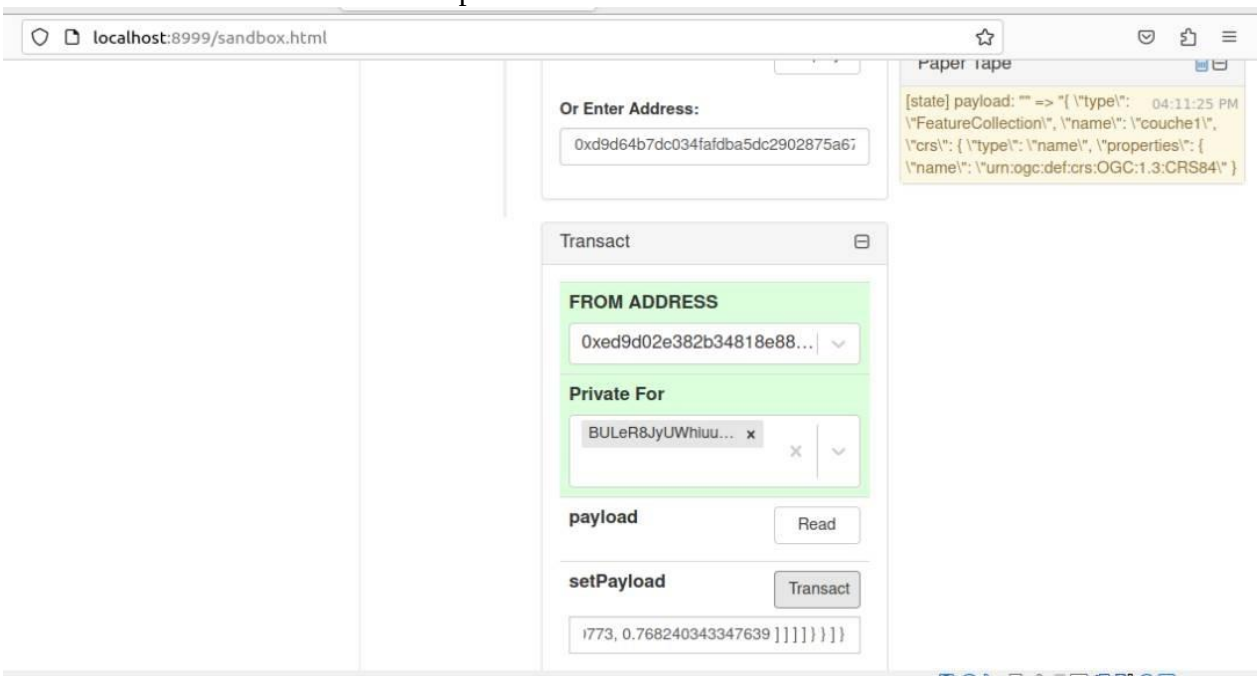


- **Création d'une transaction avec un payload constitué du GeoJSON ainsi créer**

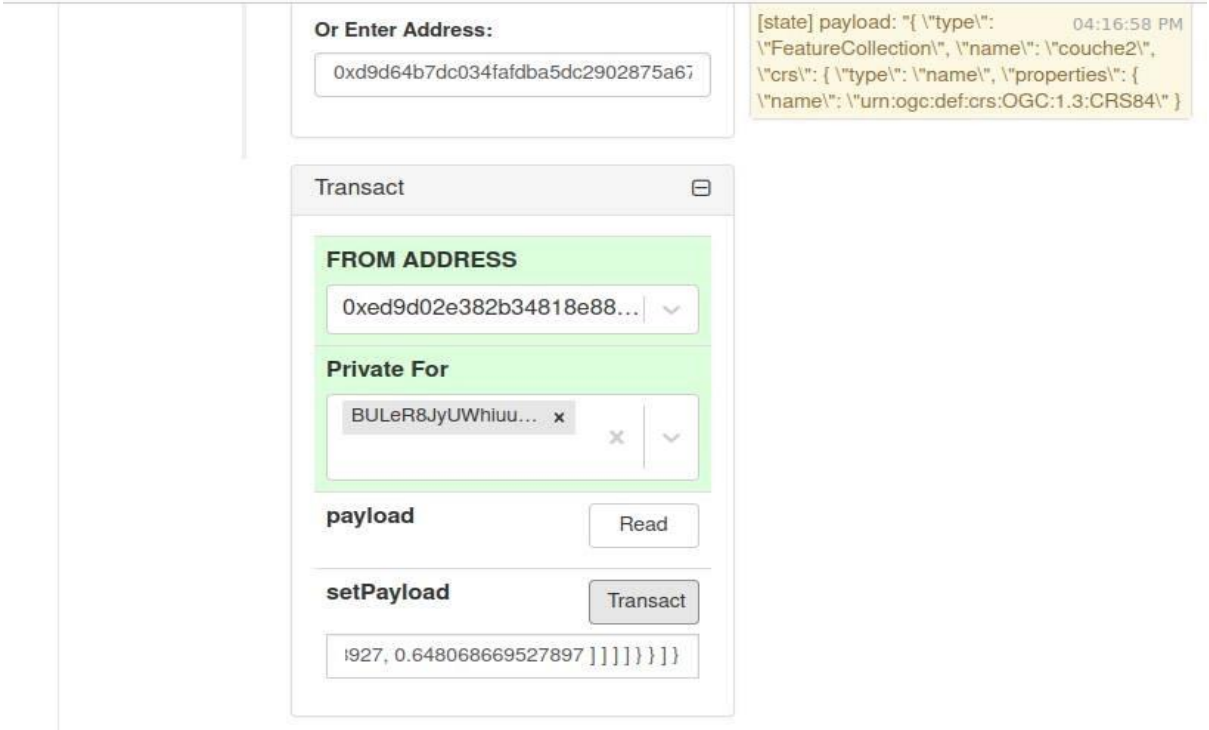
Voici le code du contrat :



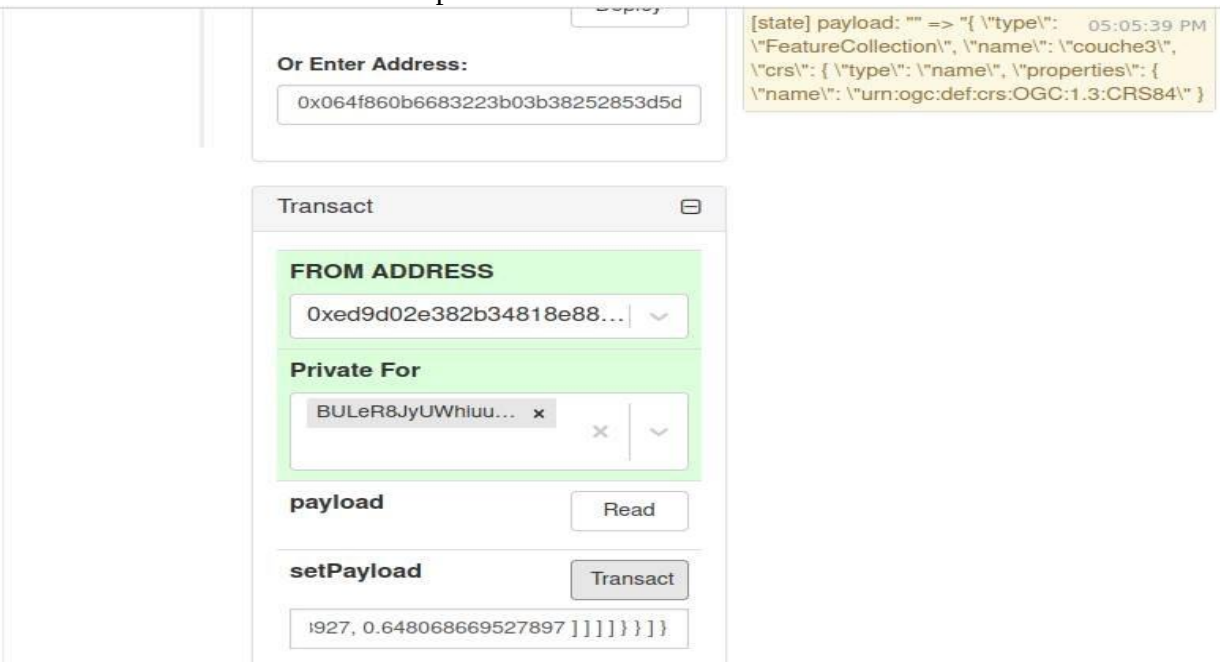
- Transaction pour la couche 1



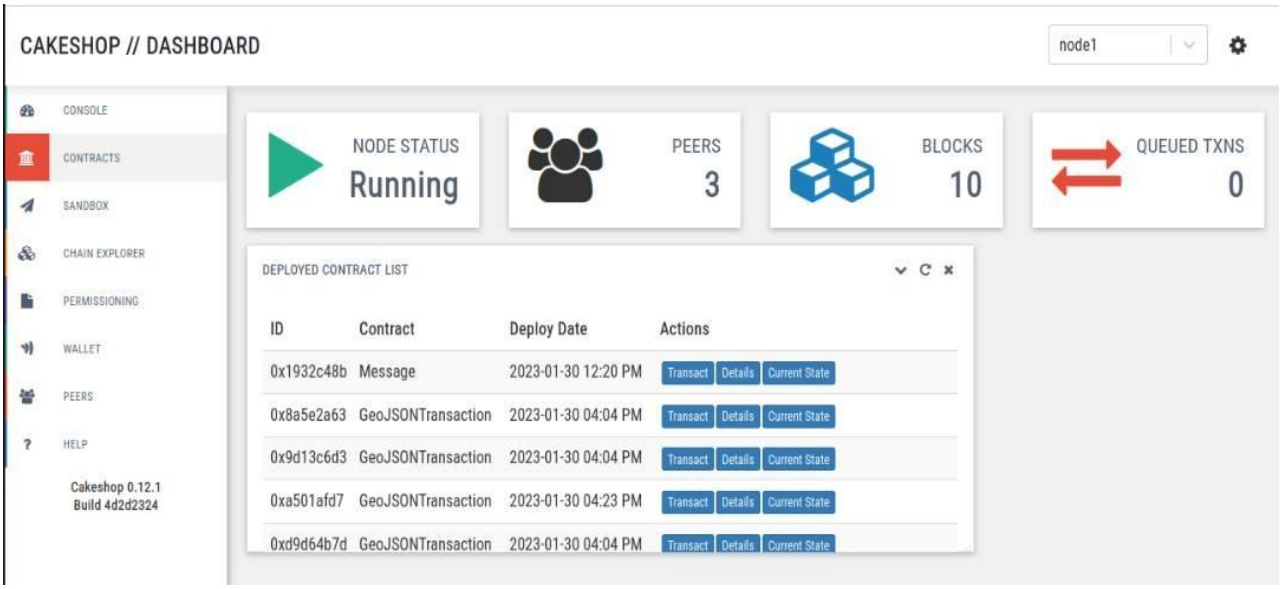
- Transaction pour la couche 2



- Transaction pour la couche 3



Ci-dessous nous avons les transactions créées :



- **Création d'une transaction avec un payload constitué du hash de la parcelle à 4 sommets :**