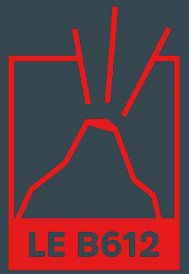
Saison printemps : Decentralized Infrastructure

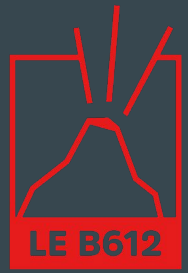
•••

Oracles décentralisés



Meetups B612 Crypto Lyon

- Série de meetup initié François Guezengar (Dapps nation)
- A venir, saison Printemps/été animé par:
  - François Branciard
  - Vladimir Ostapenco



Saison Printemps : Decentralized Infrastructure

- **Oracles décentralisés**
  - **B612 - 22/05/2019**

- Infrastructure decentralisée avec le DAppNode
  - B612 - 29/05/2019

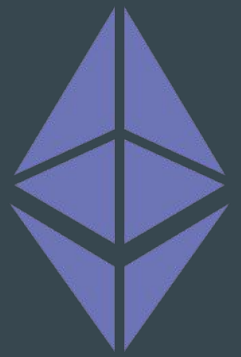
- Déployez votre site web de manière décentralisée et inarrêtable
  - B612 - 05/06/2019

Aujourd'hui

- Introduction Ethereum
- Pourquoi les Oracles?
- Oracles avec iExec
  - Presentation d'iExec
  - Architecture
  - Demo: Price feed
- Autres Use Cases
- Open mic : Vos questions et idées

Introduction Ethereum

- Une chaine de bloc
- Des blocs contenant des transactions
- Consensus pour creer ces block (PoW now)
- Des transactions pour envoyer de la valeur (ETH), mais pas que.
- Des transactions pour stocker du code (smart contract)
- Des transactions pour appeler des fonctions de ces smart contracts.
- Ces fonctions de smart contract peuvent être appelé par :
  - Des gens (des wallets)
  - D'autres smart contracts
  - Des oracles (des wallets in finé)
- Turing-complet gasifié



C’est quoi les Oracles?

- Base de données?

ORACLE

- L’album de Miserycorde?

- Une personne fournissant des prédictions prophétiques ou une précognition du futur, inspirées par les dieux?

Un peu ça oui, mais dans notre société moderne, on préféra plutôt :

- Une connaissance aidant à prendre une bonne décision
- Une information externe permettant un changement d’état

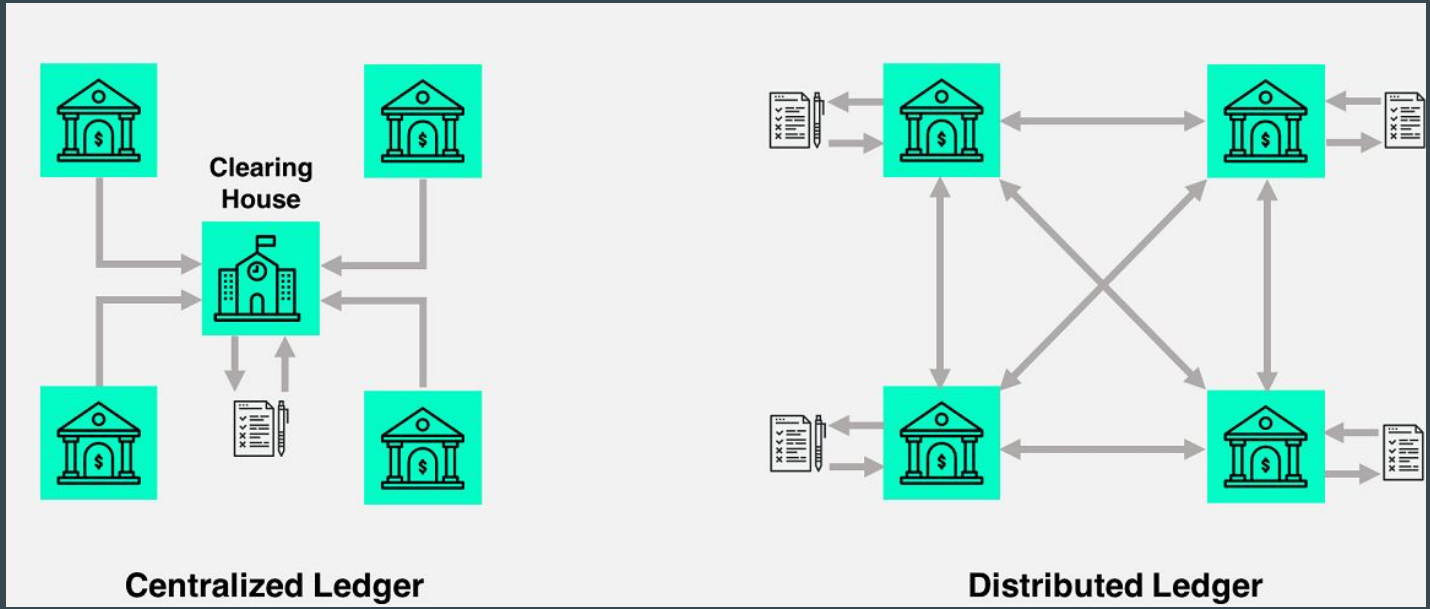
Decentralized oracles

I. Qu'est ce qu'un oracle, quel besoin?
   A. Blockchain/DLT
   B. Ethereum/Smart contracts
   C. Connection problem

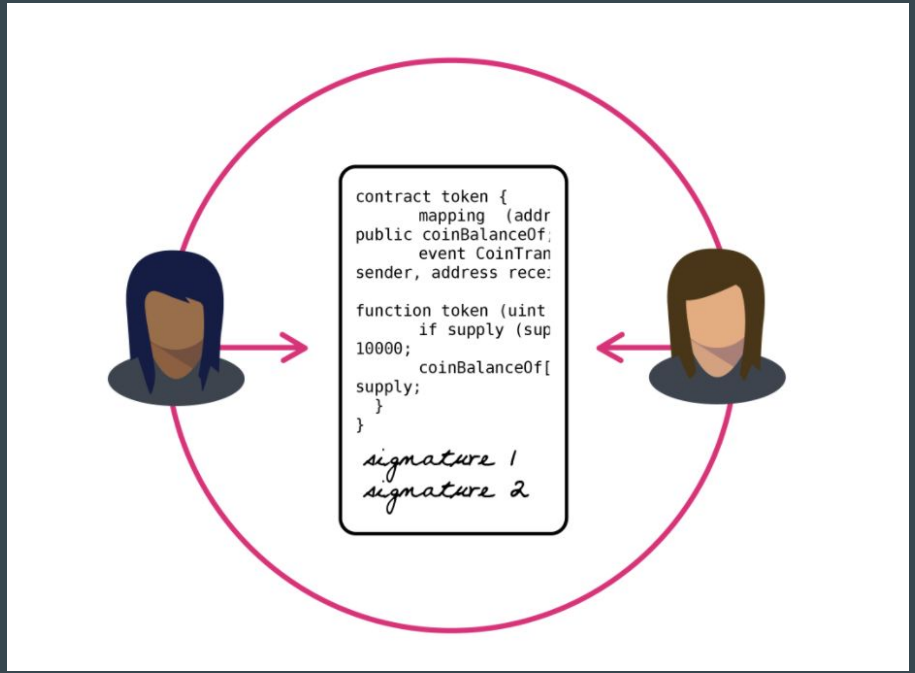
II. La solution iExec
   A. Architecture d'iExec
   B. iExec dOracle: un oracle distribué
   C. Créer son propre oracle: code walkthrough

III. Démo: l'Oracle price feed

Blockchain/ Distributed ledger



Smart contract platform



Problème: les DLT sont totalement coupés du monde

- Pour qu'un smart contract soit utile, besoin de donnée du monde réel
- Résultats sportifs, données météo, information de transfert de propriété, etc...
- Comment transférer ces données dans la blockchain/le DLT?
- Exemple: smart contract de pari sportif

Problème: les DLT sont totalement coupés du monde

- Problème de définition: comment définit algorithmiquement la “bonne valeur” d’un oracle?
- Dans la pratique: utilisation des API du Web 2.0 comme proxy de la valeur recherchée
- L’ordi ne connaît pas “résultat du dernier match NBA”...
- ... mais il connait

```
unirest.get("https://api-nba-v1.p.rapidapi.com/games/gameId/100")
```

Problème sécurité

- Le smart contract ne peut pas appeler l'API lui-même; seulement recevoir un message et lire des valeurs d'autres smart contract
- Envoi de la valeur de l'API par message
- Problème: besoin d'un tiers de confiance

La solution: décentralization + random sampling

- Un pool d'agents pour faire les requête API et forwarder le résultat
- Pour chaque requête, choisir un petit nombre d'agent au hasard
- Un attaquant doit contrôler un énorme nombre d'agent pour modifier le résultat

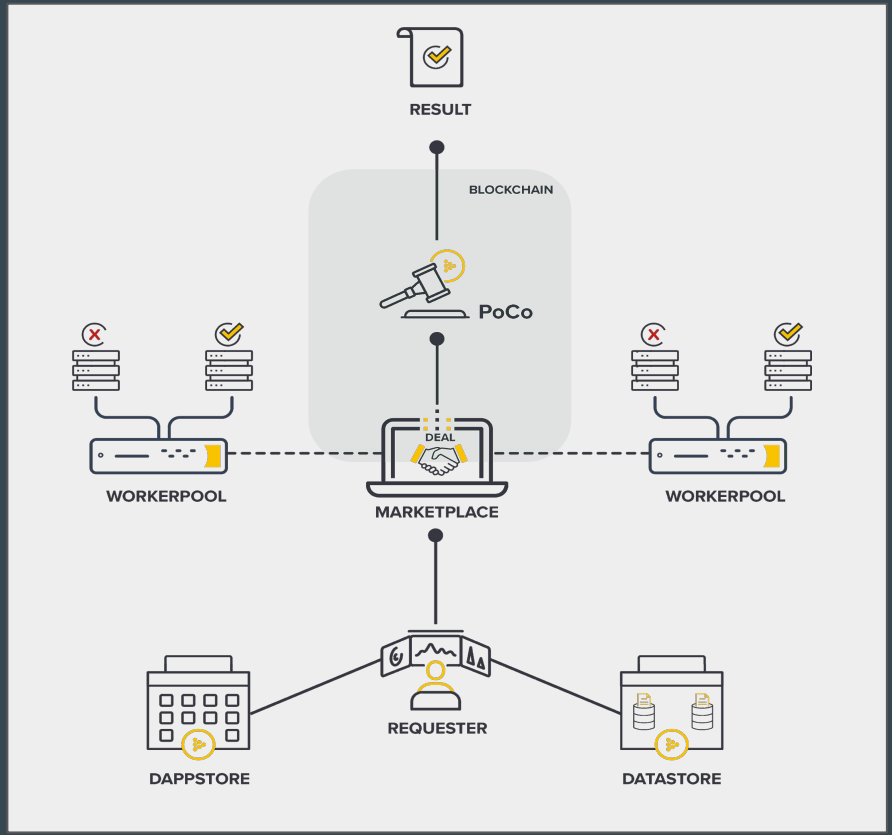
Comment implémenter dans la pratique?

- Besoin d'un grand nombre d'agent indépendants prêt à exécuter un script arbitraire
- Besoin d'un système de rémunération et de punition pour les agents.
- Besoin d'une infrastructure complète, facile à utiliser pour les développeurs, et intégrée avec la blockchain
- Besoin de ....

iExec: decentralized cloud computing

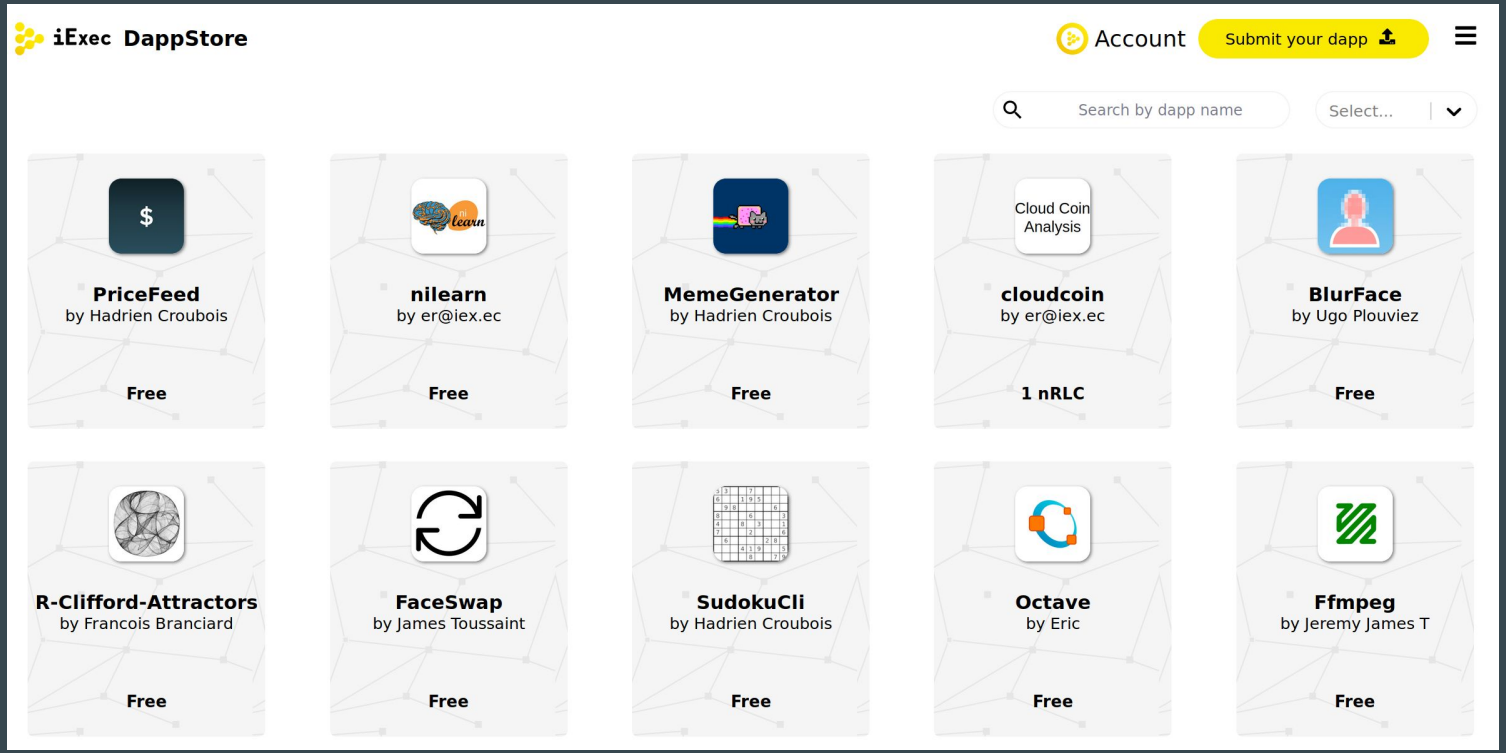
- Fondé en 2016
- Cloud computing marketplace
- Infrastructure complètement adaptée pour le développement d'Oracles

The iExec platform: architecture



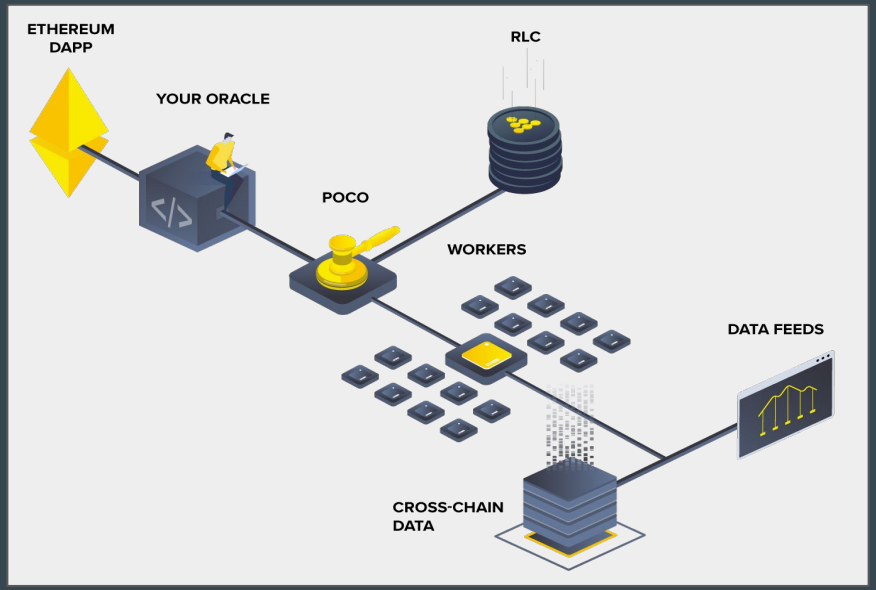
The iExec platform: the marketplace

The iExec platform: the dApp store



iExec dOracle: comment ça marche?

- Deux partie: une app normale, répliquée sur plusieurs workers, qui appelle l'API et contribue le résultat sur la blockchain, et un smart contract qui s'update avec le résultat



Code walkthrough: the API caller app

```
14  const query = {
15          method: 'GET',
16          port:   443,
17          host:   'rest.coinapi.io',
18          path:   `/v1/exchangerate/${asset_id_base}/${asset_id_quote}?time=${time}`,
19          headers: {'X-CoinAPI-Key': '69CC0AA9-1E4D-4E41-806F-8C3642729B88'},
20  };
21
22  new Promise(function (resolve, reject) {
23          var request = https.request(query, function (response) { response.on("data", resolve) });
24          request.on('error', reject);
25          request.end();
26  })
27  .then(data => {
```

Code walkthrough: the dOracle smart contract

```
50          function processResult(bytes32 _oracleCallID)
51          public
52          {
53                  uint256       date;
54                  string memory details;
55                  uint256       value;
56
57                  // Parse results
58                  (date, details, value) = decodeResults(_iexecDoracleGetVerifiedResult(_oracleCallID));
59
60                  // Process results
61                  bytes32 id = keccak256(bytes(details));
62                  if (values[id].date < date)
63                  {
64                          emit ValueChange(id, _oracleCallID, values[id].date, values[id].value, date, value);
65                          values[id].oracleCallID = _oracleCallID;
66                          values[id].date         = date;
67                          values[id].value        = value;
68                          values[id].details      = details;
69                  }
70          }
71  }
```

Demo price feed

- Demo price feed
  - https://price-feed-doracle.iex.ec/
  - https://kovan-pool.iex.ec/
  - https://explorer.iex.ec/

- Demarrer worker iExec
  - https://jupiter-pool.iex.ec

Autres Use Cases

- Une source de random
  - Jeux
  - Casino
- Les valeurs des API
  - Resultats des matchs
    - Paris sportif (exemple social bet)
  - Assurance
    - Vol annulé ou retardé
    - Meteo (pour les agriculteurs) (géle ou intemperie)
- Autres ? :
  - Oracle décentralisé => La “française des Gueux“: du Pain et des jeux par le peuple pour le peuple

Open mic : Vos questions et idées sur les Oracles