



Diplôme d'ingénieur en Télécommunications, Services et Usages

Rapport de stage de 5<sup>e</sup> année

Période du 21/02/2022 au 19/08/2022

---

*Évaluation de la migration du client  
OpenEthereum d'une sidechain EVM en  
production*

---

Tuteur enseignant : M. Damien Reimert  
INSA Lyon – Département  
Télécommunications, Services et  
Usages  
6 Avenue des Arts  
69100 Villeurbanne

Maitre de Stage : M. Zied Guezmi  
iExec  
25 Rue Jules Valensaut  
69008 Lyon - France



## Table des matières

<i>Remerciements</i> .....	4
1. <i>Contexte et sujet du stage</i> .....	5
2. <i>Entreprise : Activité et positionnement économique</i> .....	6
a. Présentation de l'entreprise .....	6
b. Partenaires et fournisseurs .....	6
c. Stratégie de développement marketing, commercial, communication.....	6
d. Concurrents directs et indirects : .....	7
Matrice SWOT .....	8
3. <i>Missions abordées</i> : .....	9
a. Se familiariser avec les concepts de base de la blockchain .....	9
i. Concepts de base de la blockchain .....	9
ii. Ethereum, au-delà d'un registre partagé.....	11
b. Prise en main de la stack technologique d'iExec.....	16
c. Utiliser OpenEthereum pour construire une chaîne locale iso à Bellecour .....	18
d. Choix du nouveau client et test de migration .....	23
e. Diagramme de Gantt de mon stage.....	25
4. <i>Thèmes SHS</i> .....	25
a. Qu'est-ce qu'une ICO ? .....	26
b. Quels sont les avantages et les inconvénients de procéder à une ICO ? .....	27
c. Impacts de l'ICO sur iExec .....	28
5. <i>Métier et projet professionnel</i> .....	29
a. Composition interne et méthodes de management .....	29
b. Mon métier d'ingénieur pendant le stage .....	30
c. Étape dans mon projet professionnel.....	30
6. <i>Retour d'expérience personnel</i> .....	31
7. <i>Conclusion générale</i> .....	32
<i>Table des sigles et des abréviations</i> .....	33
<i>Bibliographie</i> .....	33
Figure 1. Matrice SWOT.....	8
Figure 2. Processus de transaction <a href="https://www.investopedia.com/terms/b/blockchain.asp">https://www.investopedia.com/terms/b/blockchain.asp</a> .....	10
Figure 3. Diagram de la Machine d'état EVM <a href="https://ethereum.org/en/developers/docs/evm/">https://ethereum.org/en/developers/docs/evm/</a> .....	11
Figure 4. Equivalence entre architecture du Web 2.0 et du Web 3.0 .....	12
Figure 5. Architecture du Web3 .....	12

Figure 6. Crypto Zombies.....	13
Figure 7. Roadmap de Oliver Jumpertz.....	13
Figure 8. Page d'accueil et console d'Ethernaut.....	13
Figure 9. Tous les logiciels nécessaires avec Truffle .....	14
Figure 10. Logo de Hardhat .....	14
Figure 11. Diagramme UML des smart contracts .....	15
Figure 12. Schéma d'interaction entre utilisateurs et smart contracts .....	15
Figure 13. Schéma des droits sur les portefeuilles .....	15
Figure 14. Web application de la Dapp.....	16
Figure 15. Diagramme UML des acteurs et interactions du PoCo .....	17
Figure 16. Première architecture d'une blockchain de test.....	19
Figure 17. Architecture du fichier chain-spec.json .....	19
Figure 18. Enregistrement des 3 clefs par le Key-Manager .....	20
Figure 19. Génération des clefs initiales.....	20
Figure 20. Architecture final à la fin de la cérémonie.....	20
Figure 21. Résumé présent pour une adresse sur l'explorateur de bloc .....	21
Figure 22. Application web du bridge.....	22
Figure 23. Application web pour la gestion des votes .....	22
Figure 24. Résumé des étapes à suivre pour le déploiement d'une blockchain locale .....	23
Figure 25. Liste des différents clients Ethereum .....	23
Figure 26. Message d'erreur de synchronisation .....	24
Figure 27. Diagramme de Gantt du stage.....	25
Figure 28. Aperçu du wallet multi-signature d'iExec .....	27
Figure 29. Composition interne d'iExec .....	29

## Remerciements

Je voudrais remercier Damien Reimert qui a piqué ma curiosité en nous introduisant la notion de Blockchain en 2020.

Je voudrais remercier Zied Guesm, mon tuteur de stage, qui a su me transmettre son savoir et sa passion tout au long de mon stage. Sans sa bienveillance, je n'aurais pas pu autant avancer dans mon projet professionnel. Travailler avec lui a été un réel plaisir.

Je voudrais également remercier Oleg Lodygensky, Gilles Fedak ainsi que toute l'équipe Technique du deuxième étage d'iExec qui m'ont accueilli et accompagné chaleureusement au travers de ces 6 mois. Chacun s'est porté volontaire pour répondre à mes questions techniques.

Je voudrais généralement remercier toutes les personnes que j'ai pu rencontrer dans la iMaison. Merci pour votre accueil et votre sympathie ainsi que pour les tous les moments et évènements agréables que nous avons pu partager dans les locaux.

## 1. Contexte et sujet du stage

Ce rapport est le rendu final de mon stage de fin d'études encré dans la dernière année d'études de mon cursus en Télécommunications, Services et Usages à l'INSA de Lyon. J'ai eu l'opportunité d'effectuer mon stage entre le 21 février et le 19 aout 2022 dans l'entreprise blockchain iExec.

L'entreprise iExec est l'un des pionniers du Cloud décentralisé. À la suite de leur ICO de 2017, ils ont réussi à combiner la Blockchain et le Cloud pour mettre en place la première place de marché décentralisée permettant de monétiser des serveurs, des applications et des données sur la Blockchain Ethereum.

Cette place de marché fonctionne sur les blockchains de type EVM, c'est pourquoi iExec a mis en place deux blockchains : une blockchain de production Bellecour et une blockchain de test Viviani. Ces deux blockchains sont maintenues par iExec, et c'est pour l'instant, elle qui la maintient fonctionnelle et à jour. Chaque nœud validateur de ces Blockchains doit faire tourner un client Ethereum : celui-ci est essentiel pour le fonctionnement de la blockchain, communication, minage, etc. Tout est géré grâce au client.

Le client jusqu'à présent est OpenEthereum [1]. Celui-ci est maintenant déprécié depuis juin 2020 [2]. Pour continuer de maintenir active les Blokchains, il est alors nécessaire de migrer vers un nouveau client. Il en existe plusieurs, mais tous ne proposent pas les mêmes fonctionnalités. Sachant que les blockchains d'iExec implémentent l'algorithme de consensus de preuve d'autorité, il faut donc trouver un client qui est compatible avec les produits d'iExec.

L'objectif de mon stage est ainsi d'étudier et de proposer un nouveau client compatible avec la sidechain. Celle-ci permet de faire tourner les applications d'iExec. Pour mener à bien cet objectif, je vais devoir au préalable prendre en main toute la technologie Blockchain et les produits d'iExec. C'est ensuite que je serais amené à étudier les nouvelles possibilités permettant de faire évoluer la blockchain d'iExec.

## 2. Entreprise : Activité et positionnement économique

### a. Présentation de l'entreprise

iExec est une start-up blockchain fondée en 2016 et basée à Lyon. L'entreprise développe la première place de marché décentralisée pour les ressources informatiques, permettant de monétiser l'usage de ses serveurs, de ses jeux de données et de ses applications. iExec utilise la blockchain Ethereum pour organiser les échanges sur la place de marché en apportant gouvernance, confiance et sécurité. S'appuyant sur la Blockchain et le Confidential Computing, la solution d'iExec assure la gouvernance et la confidentialité des données, tout en garantissant la confiance sur l'exécution des tâches de calcul. L'entreprise dispose de sa propre crypto-monnaie, le RLC. iExec propose également une offre de consulting et d'accompagnement aux entreprises sur les projets Blockchain, de la phase d'idéation jusqu'au déploiement. Elle accompagne donc les entreprises dans le développement de projets blockchain, mais aussi entretient des liens étroits avec le monde de la recherche.

Gilles Fedak, Haiwu He et Oleg Lodygensky ont fondé iExec en 2016 après la sortie de la première version de leur livre blanc le 3 septembre 2016. Ils ont choisi, en avril 2017, d'effectuer une campagne de financement par le biais d'une ICO (initial coin Offering) en émettant leur jeton numérique (RLC) en échange de financement. Celle-ci s'est placée comme l'ICO majeur de France en 2017, en levant 12 M \$ en quelques minutes. L'équipe iExec a délivré le produit initial après trois ans. Maintenant, la startup compte à peu près 40 employés. Ces employés sont répartis autour de différents pôles : business, communication, tech et recherche. L'entreprise accueille aussi des thésards.

iExec développe et propose divers produits. Ils ont conçu le jeton numérique, le RLC, qui est un jeton de gouvernance. Il s'utilise comme méthode de paiement lors de l'utilisation du réseau iExec. Ce jeton va avoir une place dans le fonctionnement de la place de marché décentralisé d'iExec. Il y a aussi des produits permettant la création d'oracle de manière décentralisée et automatique. Ces oracles établissent un pont entre le monde réel et les produits cloisonnés présents sur la blockchain. Finalement, iExec développe des bibliothèques et des outils open-source permettant aux projets de tirer pleinement parti du cloud décentralisé. Comme expliqué brièvement, iExec propose aussi une solution de business, un service de B2B en tant que consultant pour apporter son expertise dans le domaine de la blockchain.

### b. Partenaires et fournisseurs

iExec est notamment partenaire d'Intel, IBM Cloud, Google Cloud, NVIDIA... L'entreprise est engagée dans plusieurs projets Blockchain à l'échelle européenne. L'entreprise est notamment membre de OnToChain qui est un projet lancé par la Commission européenne via l'initiative Next Generation Internet. iExec, en tant que membre, soutien les innovateurs (universitaires et entreprises de haute technologie) dans la conceptualisation, le développement, l'expérimentation et l'intégration de nouvelles technologies de blockchain et de grands livres distribués qui visent à préserver l'intégrité et la fiabilité des informations et du contenu.

### c. Stratégie de développement marketing, commercial, communication

La stratégie de communication d'une entreprise se basant sur un produit blockchain est très intéressante. En effet, dans ce type d'entreprise, la relation avec le public et la communauté est très mise en avant. Ce sont souvent ces derniers qui font vivre le projet, comme ce sont eux qui sont au cœur de l'investissement. iExec se doit donc d'être en communication permanente avec cette

communauté d'investisseurs. C'est pour cela qu'iExec possède une équipe de responsables des communautés occidentales et asiatiques. Les cofondateurs ont une image publique très importante, ils participent hebdomadairement à des conférences et sont fréquemment conférenciers.

La communication d'iExec se fait par le biais de différents canaux de réseaux sociaux : Twitter, Slack, Telegram, Youtube, mais aussi par l'écriture d'articles Medium. Lorsqu'un nouveau produit est sur le point de sortir, il y a habituellement l'écriture d'une vidéo Youtube présentant le produit, ainsi qu'un article Medium détaillant son fonctionnement.

iExec propose une solution B2B, c'est-à-dire business to business, c'est le modèle commercial qui se concentre sur la vente de produits et de services d'une entreprise à une autre entreprise. iExec aide les organisations professionnelles dans l'élaboration de projets blockchain et le fait en trois étapes : découverte et idéation, et ensuite transformation des idées en PoCs et en produit. Pour trouver de nouveaux clients business, iExec est habituellement présent aux divers salons d'innovations, autour des enjeux de la blockchain, de la confidentialité des données. Cela permet à iExec de se présenter aux grands comptes et de présenter leurs produits et services.

Un autre point intéressant concernant la communication d'iExec, c'est la mise en place d'un système de subvention. Depuis un an, il existe un programme qui alloue 1 million de dollars pour inciter les développeurs à découvrir les possibilités d'innovation rendues possibles par le protocole iExec. Ces systèmes de subventions sont courants dans l'écosystème des entreprises web3. iExec à tout à gagner en fournissant ces subventions. D'un côté, cela permet de financer des travaux de développement qui favorisent l'avancement et l'adoption de leur protocole décentralisé. Deux autres systèmes de récompense sont mis en place. Le premier est pour récompenser la communauté sur les réseaux sociaux et le second une prime de bug. Tout cela est mis en place pour inciter les gens à interagir avec iExec.

#### d. Concurrents directs et indirects :

Parlons à présent des divers concurrents que peuvent rencontrer iExec. Selon moi, un des acteurs qui est en concurrence indirectement avec iExec est avant tout un fournisseur de cloud public, nous pouvons prendre l'un d'entre eux, AWS par exemple. L'utilisation des services proposés par un fournisseur de cloud est courante. Il faut donc réussir à garder et à convaincre le public à passer d'une solution centralisée à une solution décentralisée. Il faut ainsi que le produit d'iExec soit compétitif vis-à-vis de ces géants (prix, sécurité...). Il existe aussi d'autres projets qui vont être des concurrents directs d'iExec. Des projets qui comme iExec vont vouloir mettre en place des solutions de cloud décentralisé. Comme l'environnement des produits décentralisé est jeune, il y a encore peu de solutions mises en place, il est alors facile de voir quels sont les projets similaires. Nous pouvons noter :

- Filecoin et Storj Labs, Sia qui proposent une solution de stockage cloud décentralisée
- Golem qui propose une banque de puissance de calcul de machine connectée et un réseau décentralisé de performance.
- SONM construit un super-ordinateur décentralisé.

## Matrice SWOT



*Figure 1. Matrice SWOT*

iExec a choisi de se positionner sur un écosystème innovant et très jeune en proposant à leur tour un produit innovant qui est la place de marché pour de la puissance de calcul. Leur produit répond à un vrai besoin et vise un public large, ceux qui ne peuvent pas se permettre d'utiliser des services de cloud traditionnels et ceux qui veulent monétiser leur puissance de calcul inutilisé. Ils ont su réussir leur ICO en 2017. Leur jeton RLC, qui a été délivré lors de l'ICO, est soumis, comme les autres jetons numériques, à la volatilité du marché des cryptomonnaies et parfois ne représente pas la valeur du produit qu'il représente. De ce fait, on peut observer deux groupes possédants le jeton RLC, les investisseurs initiaux et les nouveaux détenteurs.

Le domaine de la blockchain est tout aussi volatil en matière d'investissement qu'en matière d'innovation. C'est-à-dire que de nouveaux produits voient le jour quotidiennement. Si iExec ne veut pas finir dans l'ombre de ces nouveaux projets, qui font parler d'eux, il faut rester le plus possible au courant et continuer de proposer des produits innovants et attrayants. L'explosion des solutions de layer deux permettant la scalabilité du réseau principal Ethereum, pourrait être un nouveau point d'ancrage pour leurs produits.

### 3. Missions abordées :

L'objectif principal du stage est de migrer le client blockchain opérant la sidechain d'iExec. Cette migration doit se faire vers un nouveau client compatible avec les applications qui fonctionnent actuellement sur la sidechain. Pour en arriver à cette fin, le stage s'est articulé autour de sept points intermédiaires. Nous allons les détailler dans ce qui suit, mais pour les citer exhaustivement :

- Se familiariser avec les concepts de base de la blockchain :
  - o La Blockchain en général & Bitcoin,
  - o Ethereum et son écosystème,
- Prendre en main la plateforme d'iExec,
- Expérimenter avec les outils de déploiement de la sidechain actuelle,
- Choisir un nouveau client Ethereum pour remplacer celui actuel,
- Expérimenter ce client sur une sidechain de test.

#### a. Se familiariser avec les concepts de base de la blockchain

Avant d'intégrer iExec il était important d'avoir déjà pu expérimenter avec le domaine de la blockchain. La formation INSA Telecom permet d'avoir des cours d'initiation en 4e année, au sujet des systèmes distribués et des cours de spécialisation en 5<sup>e</sup> année. De plus, c'est un domaine où apprendre par soi-même est très facile. C'est pourquoi depuis plus d'un an j'ai pu me rapprocher de l'écosystème pour devenir utilisateur du protocole Ethereum. De cette manière, j'ai pu avoir quelques notions de base sur le fonctionnement et les diverses possibilités que me proposait l'écosystème. Ces notions n'étaient que de surface. Pour me permettre d'avancer dans le stage, il a donc fallu que celles-ci se transforment en bagages solides de l'écosystème et du fonctionnement de la blockchain. Pour cela, je suis passé par deux étapes. La première était de reprendre les concepts de base de la blockchain en s'appuyant sur la première blockchain effective : Bitcoin. En ayant ces concepts en tête, il me sera possible de me pencher sur les bases de la blockchain Ethereum.

##### i. Concepts de base de la blockchain

Une blockchain est un grand livre de compte distribué partagé entre plusieurs nœuds d'un réseau informatique. Aux premiers abords, elle peut être comparée à une base de données distribuée, mais la structure des informations stockées est totalement différente [3]. En effet, une blockchain rassemble les informations en lots, appelés blocs. Ces blocs contiennent toutes les transactions, qui permettent au système de passer d'un état T à un état T+1. Chaque bloc s'agence comme les pages d'un livre de comptes, et chaque bloc pointe vers son bloc parent. Cela forme donc une chaîne de données appelée Blockchain.

Dans son papier blanc publié en 2008 [4], Satoshi Nakamoto annonce ce que contiennent ces blocs : une référence cryptographique du bloc précédent, un horodatage et l'ensemble des transactions, généralement représentées sous la forme d'un arbre de Merkle.

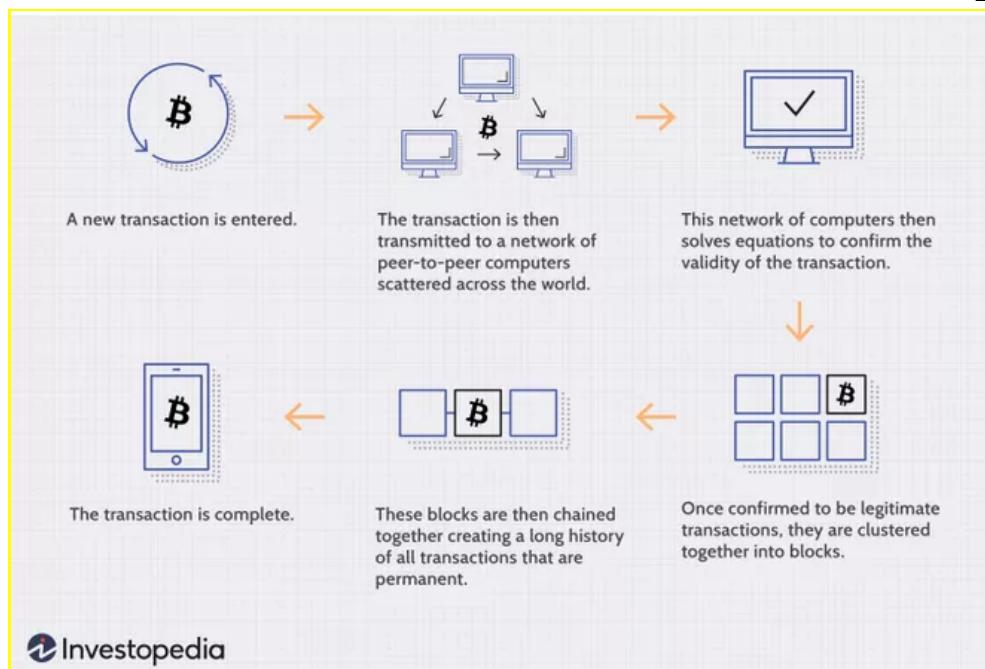


Figure 2. Processus de transaction

Après avoir défini la Blockchain, étudions le fonctionnement de la blockchain Bitcoin. Bitcoin est la première application dans le domaine de la monnaie numérique qui a réussi à subsister et qui a, donc, donné naissance au premier exemple de cryptomonnaie.

Une cryptomonnaie est une monnaie qui est totalement digitale et qui n'est contrôlée par aucun acteur central (gouvernement, banque, ...). La gestion des comptes individuels et la vérification des interactions entre les participants se font de façon décentralisée. Ainsi, Bitcoin utilise la blockchain comme un grand livre de compte partagé (distribué et répliqué) et immuable. Ce registre implique plusieurs acteurs :

- Les utilisateurs possédant un compte avec des fonds propres et pouvant s'échanger de la valeur.
- Les nœuds (nodes), qui eux vont pouvoir écrire, mettre à jour et distribuer la nouvelle version du registre.

### Le hachage

Un outil cryptographique fortement utilisé dans le domaine de la blockchain est celui de fonction de hachage. C'est une fonction mathématique qui va convertir une entrée de taille arbitraire en une sortie chiffrée de longueur fixe. Cet outil va avoir plusieurs utilités au sein de Bitcoin :

Permettre de vérifier l'intégrité des informations entre chaque bloc, Rôle central dans l'algorithme de consensus de preuve de travail.

### Le consensus

Dans ce système distribué chaque nœud du réseau pourrait ajouter un bloc à la chaîne. Dans une blockchain publique, chacun est libre de proposer un nouveau bloc avec l'ensemble de transactions qu'il souhaite. Dans ce cas, il faut pouvoir se protéger contre un individu malveillant qui tentera d'ajouter un bloc erroné. Chaque nœud voulant proposer un bloc doit au préalable réussir un défi mathématique, lui donnant l'autorisation d'écrire dans la blockchain.

Il existe plusieurs algorithmes consensus parmi lesquels :

- La preuve de travail (Proof of Work, PoW), l'enjeu de puissance de calcul : chacun doit résoudre un casse-tête basé sur la fonction de hachage sha256

- La preuve d'enjeu (Proof of Stake, PoS), l'enjeu va être monétaire : chaque nœud voulant ajouter des blocs doit mettre en gage une certaine somme d'argent. En cas de mauvais comportement, une partie de cette somme est réquisitionnée.

### ***La blockchain de iExec***

Pour faire tourner ses applications, iExec a besoin d'une blockchain. Initialement, iExec a déployé sa plateforme sur Mainnet. Mais pour des questions économiques (frais de transactions trop élevés), de performance et d'onboarding, c'est pourquoi l'entreprise a déployé sa propre blockchain et d'y déployer sa stack. Elle va elle-même sécuriser son réseau en appliquant un autre mécanisme de consensus : la preuve d'autorité. Celle-ci met en gage son identité (cas particulier de la PoS). Chaque nœud qui veut ajouter des blocs et donc devenir une autorité de la blockchain, doit dévoiler son identité publiquement. Ainsi en cas de mauvais comportement d'un nœud, des actions peuvent être menées contre l'autorité derrière. C'est un algorithme de consensus qui s'adapte parfaitement à une blockchain privée de la taille d'une entreprise.

### **ii. Ethereum, au-delà d'un registre partagé**

Vitalik Buterin a conçu la blockchain Ethereum en 2013 [5], s'inspirant des travaux de Satoshi Nakamoto sur le Bitcoin. Ethereum a été déployé le 30 juillet 2015, avec l'aide de Gavin Wood. Ethereum a été conçue comme une plateforme de contrats intelligents (cf définition en bas). La machine virtuelle Ethereum (EVM) est l'environnement d'exécution, l'endroit où les contrats intelligents s'exécutent dans Ethereum. Il fournit un langage de script plus expressif et complet que Bitcoin. En fait, c'est un langage de programmation Turing complet. Une bonne analogie est que l'EVM est un ordinateur mondial distribué où tous les contrats intelligents sont exécutés.

Chaque opération effectuée dans l'EVM est en fait effectuée simultanément par chaque nœud du réseau, les ressources sont donc limitées. C'est pourquoi le concept de "Gas" a été inventé [6]. Toute transaction à un coût mesuré en gaz, et chaque unité de gaz consommée par la transaction doit être payée en "Ether", la cryptomonnaie de la blockchain Ethereum, sur la base de l'évolution dynamique du prix du gaz/Ether.

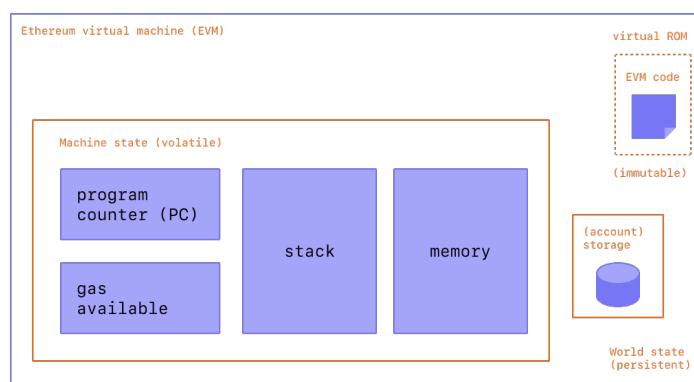


Figure 3. Diagram de la Machine d'état EVM

Cette définition d'Ethereum introduit beaucoup de notions importantes.

Chaque bloc d'Ethereum contient une liste de transactions qui modifiera l'état global d'Ethereum d'un état T à un état T+1. Ces transactions sont spécifiques et contiennent des variables comme le destinataire, la signature, la donnée envoyée, le montant en \$ETH transféré, et les informations relatives au gaz.

### **Les smart contract**

Un "contrat intelligent" est un programme qui s'exécute sur la blockchain Ethereum. Il s'agit d'un ensemble de codes et de données situés à une adresse spécifique sur la blockchain Ethereum. Un contrat intelligent est un type de compte Ethereum. Cela signifie qu'ils ont un solde et peuvent envoyer des transactions sur le réseau (mais pas les initier). Cependant, ils ne sont pas contrôlés par l'utilisateur, ils sont déployés sur le réseau et s'exécutent comme des programmes. Les comptes d'utilisateurs peuvent ensuite interagir avec les contrats intelligents en soumettant des transactions qui exécutent des fonctions définies dans le contrat intelligent. Comme les contrats ordinaires, les contrats intelligents peuvent définir des règles et les exécuter automatiquement par le biais du code. Par défaut, les contrats intelligents ne peuvent pas être supprimés et les interactions avec eux sont irréversibles.

### **Les applications décentralisées**

Une application décentralisée (Dapp) est une application construite sur un réseau décentralisé qui combine un contrat intelligent et une interface utilisateur, souvent Web. Ce qui distingue une dapp des autres types d'applications est que les dapps sont :

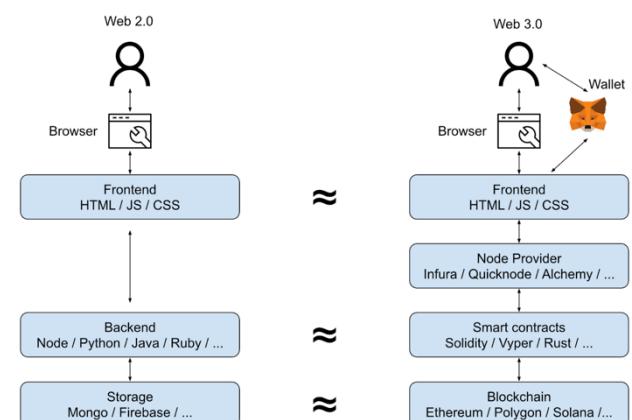
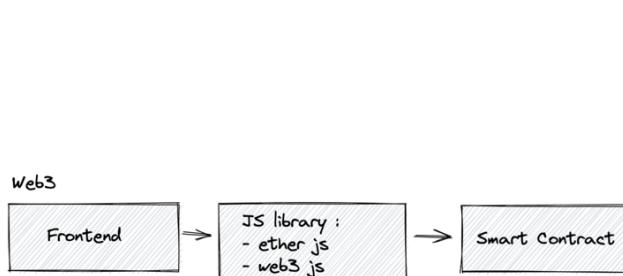
Décentralisées, contrôlées par la logique écrite dans le contrat, et non par un individu ou une entreprise

Déterministes, elles remplissent la même fonction quel que soit l'environnement dans lequel elles sont exécutées

Complets, ce qui signifie qu'ils peuvent effectuer n'importe quelle action s'ils disposent des ressources nécessaires

Isolés, ce qui signifie qu'ils sont exécutés dans un environnement virtuel connu sous le nom de machine virtuelle Ethereum, de sorte que si le contrat intelligent présente un bogue, il n'entrave pas le fonctionnement normal du réseau blockchain.

Le concept de dapp change l'architecture dans laquelle le web actuel fonctionne.



### **Solidity**

Pour construire des Dapps il faut prendre en main plusieurs outils de programmation. Le plus important est la prise en main de Solidity, le langage de programmation le plus commun pour la création de smart contract :

- C'est un langage de haut niveau, orienté objet ;
- Langage à accolades ;
- Caractéristiques : typage statique, prise en charge de l'héritage, de bibliothèque et de typage complexe définis par l'utilisateur.

Pour ce faire, il est possible de suivre la roadmap pour devenir développeur de smart contract proposée par Olivier Jumpertz [7]. Cette roadmap propose diverses ressources permettant l'apprentissage du Solidity. La ressource la plus consultée est le site interactif CryptoZombie [8]. C'est la référence pour débuter dans cet apprentissage, il permet d'avoir un large aperçu de ce que peut proposer Solidity. Pour compléter cela, la chaîne youtube Smart Contract Programmer regorge de ressources pour apprendre le Solidity et comprendre les smart contracts déployés dans les protocoles de finance décentralisé.



Figure 7. Roadmap de Oliver Jumpertz



Figure 6. Crypto Zombies

### *Les contracts intelligents et la sécurité*

Il est obligatoire d'avoir des notions sur les possibles attaques que peuvent rencontrer les smart contracts. En effet, un smart contract, une fois déployé, est immuable et il est accessible/visible par tous, ainsi s'il n'est pas testé en amont, un individu malveillant peut effectuer des attaques dessus. Les smart contracts sont souvent au cœur de protocoles de finance décentralisé, l'enjeu monétaire est très important et les attaques sont courantes impliquant souvent des centaines de millions de dollars de perte. Par exemple, en mars 2022, le réseau Ronin s'est fait attaquer [9], cela a engendré un vol de à peu près \$624M. Pour se former à la sécurité, il est possible de se renseigner auprès de Openzeppelin qui propose Ethernaut [10] qui est un CTF intégré directement dans la console de développement du navigateur.

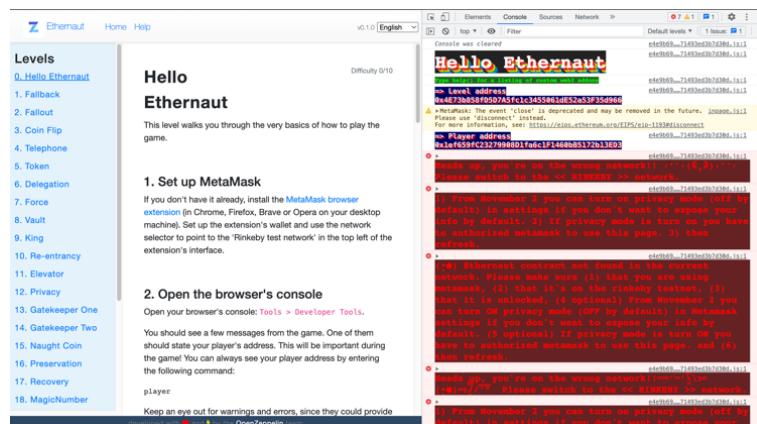


Figure 8. Page d'accueil et console d'Ethernaut

### Outils de développement

Les deux outils les plus connus sont Truffle [11] et Hardhat [12]. Les deux permettent de compiler, déployer, tester et déboguer les smart contracts. Ils proposent des outils de gestion et d'automatisation de processus.



Figure 10. Logo de Hardhat



Figure 9. Tous les logiciels nécessaires avec Truffle

Après avoir pris en main les deux, mon choix s'est porté vers l'utilisation de Hardhat et ceux pour plusieurs raisons :

- Intégration d'un réseau Ethereum de test local, Truffle a besoin d'un autre logiciel tiers : Ganache
- Utilisation de la librairie javascript Ethers Js alors que Truffle se base sur Web3 Js
- Meilleure intégration avec les fichiers de configurations, de tests et de développement.

Un autre outil très fortement utilisé pendant le stage était Git et Github. C'est le moyen de partage et de gestion de code le plus répandu dans les entreprises. C'est pourquoi tout au long du stage, j'ai pu partager des répertoires avec mon équipe. L'un d'eux est public et permet d'avoir un environnement de développement vierge avec les librairies à installer.

<https://github.com/gfournieriExec/hardhat-starter-project>

Pour résumer, plusieurs outils sont nécessaires pour le développement de smart contracts :

- Le langage de programmation des smarts contract, Solidity ;
- L'environnement de développement, Hardhat ;
- La librairie JS permettant une interaction avec la blockchain et les smart contract, Ether.js.

Afin de valider l'étape de prise en main des technologies Ethereum, il m'a été demandé de déployer une dapp, présentant ainsi mes connaissances. Pour ce faire, je me suis inspiré, d'un article écrit par Radek Ostrowski « Time-locked Wallets : An Introduction to Ethereum Smart Contracts ». Cet article propose de déployer une dapp permettant la création de portefeuilles temporisés. Pour ce faire, il y a la construction de trois smarts contracts :

- **TimeLockedWallet** : un smart contract représentant le portefeuille temporisé ;
- **TimeLockedWalletFactory** : un smart contract dit « factory », c'est en fait celui-là qui sera central car il va permettre à un utilisateur de créer une instance de portefeuille temporisé ;
- **LeirbagToken** : un smart contract de jeton ERC20 : en appliquant ce standard il est possible de créer une cryptomonnaie, celui-ci est liquide et permet par exemple de jouer le rôle de monnaie que l'on va déposer dans le portefeuille.

### Diagrammes des contrats intelligents

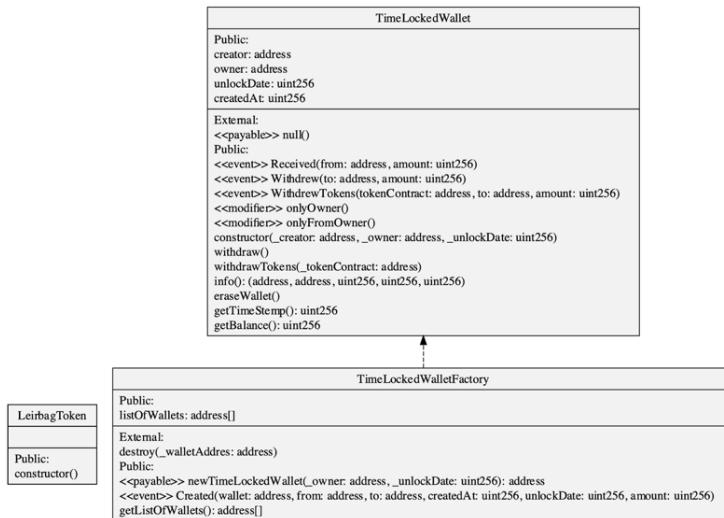


Figure 11. Diagramme UML des smart contracts

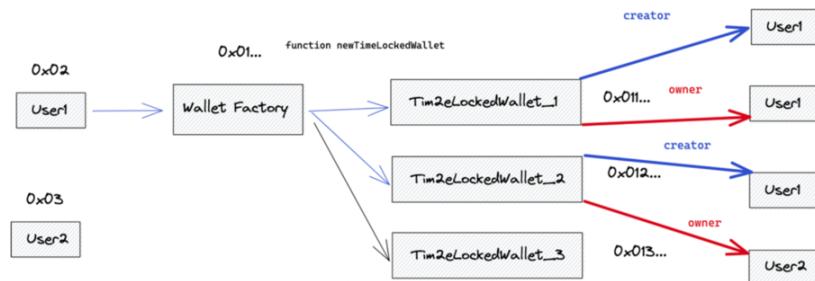


Figure 12. Schéma d'interaction entre utilisateurs et smart contracts

Ce schéma d'interactions montre les mécanismes qui relient les différents contrats intelligents  
L'utilisateur peut créer un **TimeLockedWallet** par le biais du **Wallet Factory**  
Le nouveau **TimeLockedWallet** aura un propriétaire, un créateur et une date de déblocage

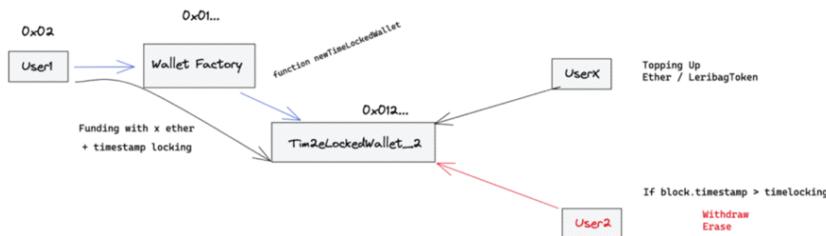


Figure 13. Schéma des droits sur les portefeuilles

Les rôles attribués déterminent les droits sur le portefeuille créé. Certaines fonctionnalités ne sont accessibles que par le propriétaire du wallet comme récupérer les fonds si la date de déblocage est passée.

L'interface utilisateur d'une Dapp permet l'interaction avec les smarts contracts et la blockchain. Pour ce point-là, j'ai construit une application web en React. Celle-ci permet 3 interactions principales avec les smarts contracts :

- Création d'un nouveau wallet
- Envoyer des fonds sur un wallet de son choix
- Récupérer les fonds d'un wallet

Lorsqu'un utilisateur se connecte à cette dapp, il obtient une liste des wallets qui ont été créés. Les différentes couleurs indiquent qui est le propriétaire du wallet

Create Wallet Contract Form									
Welcome 0x1ef659fc23279908d1fa6c1f1460bb5172b13ed3									
CONNECTED TO Your local network									
Create Wallet Contract Form									
0x1ef659fc23279908d1234   21 / 04 / 2022 11 : 07   Submit									
From	Type	To	Wallet	Age	Unlock In	Ether	Leirbag Token	Actions	Value
0x1ef659fc23279908d1fa6c1f1460bb5172b13ed3	self	0x1ef659fc23279908d1fa6c1f1460bb5172b13ed3	0xbcc667744004abb7a16869e0d9536141981b8f3	1650531615	1660031780	0	1234	Erase Wallet	
0x8876883f30000cc8410fb8943ed0120723329874	in	0x1ef659fc23279908d1fa6c1f1460bb5172b13ed3	0x4e414c223e6283890632b84ca4c13736967ce	1650532050	1660032029	0	1234	Erase Wallet	

Figure 14. Web application de la Dapp

## b. Prise en main de la stack technologique d'iExec

Afin de migrer le client qui opère actuellement la sidechain d'iExec, il faut que je prenne en main les applications qui sont déployées sur celle-ci. Cela me permettra au moment de la migration de vérifier le bon fonctionnement des applications. Il y a donc plusieurs outils à prendre en main.

- Le premier produit : la place de marché d'iExec, elle se compose notamment d'un protocole, le PoCo : Proof of Contribution ou Preuve de Contribution
- La sidechain en elle-même : il s'agit d'une blockchain EVM qui est à la base du fonctionnement de la place de marché.
- Le bridge : pont bidirectionnel qui permet d'envoyer des assets entre la sidechain d'iExec et Mainnet

Le 29 mai 2018, iExec a sorti la première place de marché de cloud décentralisé basée sur la blockchain. Elle permet d'échanger de la puissance de calcul sur un marché dédié comme n'importe quelle autre marchandise. Elle permet aux développeurs d'applications d'accéder à une puissance de calcul abordable, sécurisée et évolutive à la demande. Cette place de marché doit mettre en relation différents acteurs et ce sans tiers de confiance. Elle met entre autres en relation des fournisseurs d'applications, de data, et de puissance de calcul ainsi que les utilisateurs qui ont des nécessités auprès des différents fournisseurs. La mise en relation se fait via la place de marché. Chaque acteur va pouvoir mettre en location leurs biens et donc monétiser leurs ressources. Cela soulève plusieurs problématiques d'intégrité et de confiance. Pour ce faire, iExec a développé un protocole, le Proof of Contribution (PoCo) qui vérifie chaque calcul hors chaîne exécuté. De plus, il y a des questions sur la confidentialité des calculs, c'est pourquoi iExec utilise les environnements Trusted execution environment (TEE) dont Intel Software Guard Extensions (Intel SGX), mais cela ne rentre pas spécifiquement dans la portée de mon stage.

### Le PoCo

Ce protocole a été conçu pour permettre d'arriver à un état de confiance dans un environnement décentralisé. Elle doit s'établir entre les trois agents qui vont avoir recours au produit : les fournisseurs d'applications, les utilisateurs et les « workers » : ce sont les ressources de calculs. Il faut pouvoir se protéger contre les « workers » qui pourraient fournir de mauvais résultats, mais aussi des utilisateurs

qui pourraient contester le travail légitime effectué par des workers légitimes. Pour ce faire, plusieurs idées vont être mises en place :

- Mettre en place une incitation financière
- Atribuer à chaque « workers » un niveau de réputation

Les workers vont s'enregistrer auprès d'un « scheduler » et travailler par groupes (architecture master/slave). Lorsqu'un utilisateur va soumettre une tâche au scheduler, ce dernier va attribuer le travail à exécuter à un ou plusieurs workers. Après avoir effectué le calcul demandé, chaque worker soumet son résultat sur la blockchain. Un vote est établi pour savoir si le résultat d'un worker est bon. Si ce n'est pas le cas, le worker va perdre une partie de son capital et de sa réputation. A contrario, le scheduler et les bons workers vont se partager le pot qui regroupe les amendes des mauvais workers et le paiement de l'utilisateur pour la tâche. De plus, la réputation des workers augmentera.

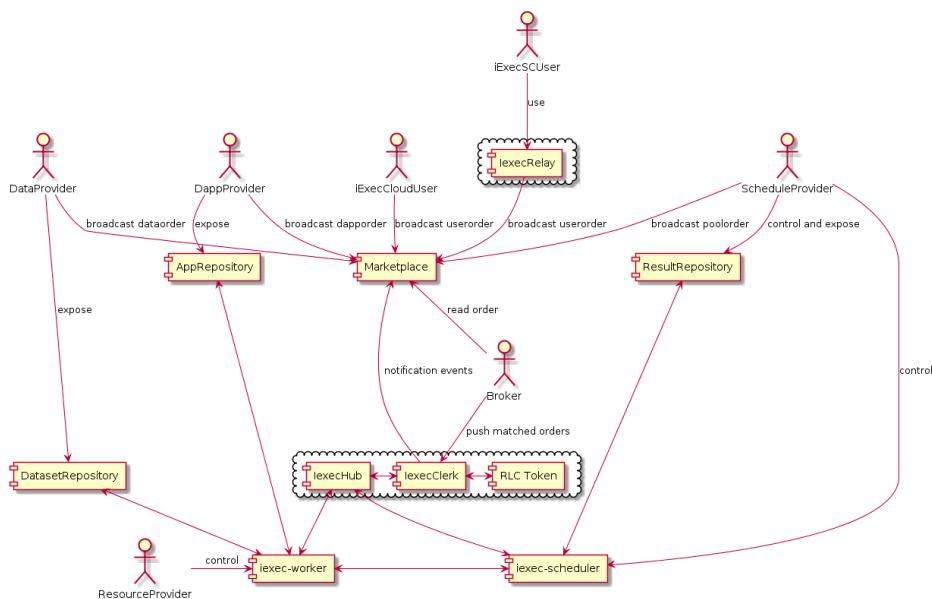


Figure 15. Diagramme UML des acteurs et interactions du PoCo

Actuellement, la place de marché et le consensus sont déployés sur les blockchains Mainnet, Bellecour et Viviani. Le répertoire GitHub permettant de déployer le protocole PoCo : [iExecBlockchainComputing/PoCo](#), il contient tous les fichiers de tests, déploiement des smart contracts, etc. Nous reviendrons sur ce protocole, mais pour vérifier le bon fonctionnement du déploiement, il faut pouvoir déployer une application sur le protocole et vérifier que l'on peut l'exécuter.

#### *La blockchain d'iExec, la sidechain*

Pour présenter une blockchain, il y a différents points à énoncer.

- De quel type de blockchain s'agit-il ?
- Quel est le client qui fait tourner la blockchain
- Quelques statiques
- Quel est l'algorithme de consensus ?
- Combien il y a-t-il de participants au réseau

Nous allons recueillir ces informations dans un tableau. L'entreprise iExec a déployé deux blockchains : Bellecour et Viviani. Viviani est le réseau de test et Bellecour la sidechain de production. Une sidechain est une blockchain distincte qui fonctionne indépendamment d'Ethereum et qui est connectée à une autre blockchain par un pont bidirectionnel qui permet de transférer des assets digitaux.

Informations	Bellecour	Viviani
Quel type de blockchain ?	Compatible EVM, sidechain, réseau privé	Compatible EVM, sidechain, réseau privé
Comment s'y connecter à l'aide de Metamask ?	<b>Network Name</b> ⓘ iExec Sidechain <b>Network URL</b> ⓘ <a href="https://bellecour.iex.ec">https://bellecour.iex.ec</a> <b>Chain ID</b> ⓘ 134 <a href="#">View all details</a>	<b>Network Name</b> ⓘ iExec Test Sidechain <b>Network URL</b> ⓘ <a href="https://viviani.iex.ec">https://viviani.iex.ec</a> <b>Chain ID</b> ⓘ 133 <a href="#">View all details</a>
Algorithme de consensus	PoA: Proof of Authority - AuRa	PoA: - AuRa
Client qui opère la blockchain	OpenEthereum	OpenEthereum
Nombre de nœuds validateurs	8	5
Explorateur de blocs	<a href="https://blockscout-bellecour.iex.ec/">https://blockscout-bellecour.iex.ec/</a>	<a href="https://blockscout-viviani.iex.ec/">https://blockscout-viviani.iex.ec/</a>
Nestat : monitoring de la chaîne	<a href="https://netstat-bellecour.iex.ec/">https://netstat-bellecour.iex.ec/</a>	<a href="https://netstat-viviani.iex.ec/">https://netstat-viviani.iex.ec/</a>
dApp de vote	<a href="https://voting-bellecour.iex.ec/poa-dapps-voting">https://voting-bellecour.iex.ec/poa-dapps-voting</a>	<a href="https://voting-viviani.iex.ec/poa-dapps-voting/">https://voting-viviani.iex.ec/poa-dapps-voting/</a>
Bridge	<a href="https://bridge-bellecour.iex.ec/">https://bridge-bellecour.iex.ec/</a>	<a href="https://bridge-viviani.iex.ec/">https://bridge-viviani.iex.ec/</a>
Fréquence d'émission de bloc	5 secondes	5 secondes
Frais de Gas	0 Gwei (transactions gratuites)	0 Gwei

### c. Utiliser OpenEthereum pour construire une chaîne locale iso à Bellecour

Le but de mon stage est de proposer une migration du client OpenEthereum qui est actuellement le client Ethereum qui fait tourner les blockchains d'iExec. Le 2 juin 2021, l'équipe qui était à la tête du développement du client OpenEthereum a décidé de ne plus y toucher et de se concentrer sur celle du client Erigon. Étant déprécié, il faut alors trouver le client qui va pouvoir remplacer OpenEthereum. Cela impose quelques contraintes :

- Il faut que le futur client puisse implémenter l'algorithme de consensus de Bellecour
- Vérifier la compatibilité des applications qui sont d'ores et déjà déployé sur la sidechain
  - o PoCo
  - o Les smarts contracts de consensus PoA
  - o Les dApps présentés plus haut, reliées aux smarts contracts
  - o Le bridge

Afin de préparer les tests sur un nouveau client, il m'a été demandé de reconstruire la sidechain Bellecour actuelle, avec les applications déployées. Ainsi, en ayant un réseau identique à Bellecour, je n'aurais qu'à changer de client et à faire mes tests. Pour ce faire, il a donc fallu que je déploie une blockchain de test de manière locale avec l'aide du client OpenEthereum et de Docker.

Avant de me lancer dans le déploiement d'une blockchain de la taille de Bellecour, j'ai d'abord créé un réseau avec trois nœuds : deux validateurs et un full node et sur celui déployé la Dapp précédemment mentionnée.

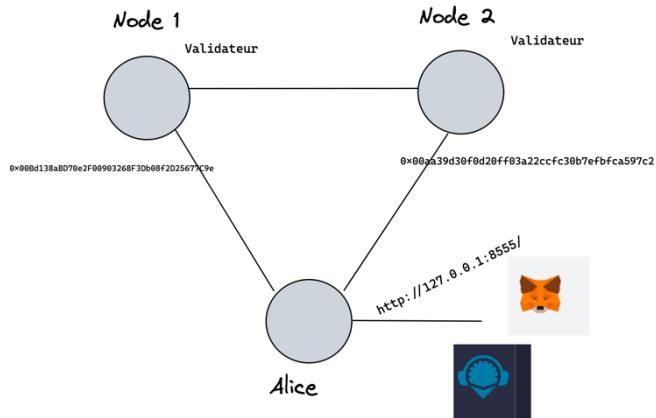


Figure 16. Première architecture d'une blockchain de test

#### Construire une architecture similaire à celle présente sur Bellecour.

Plusieurs étapes sont à reproduire pour déployer une blockchain de la sorte : création du bloc de genèse, la cérémonie, déploiement du protocole PoCo, déploiement d'un « bridge ».

Toute blockchain doit commencer par un bloc de genèse, c'est le premier bloc qui est émis lors de la création d'un réseau. Celui-ci est indiqué dans le fichier de configuration de la chaîne ([chain-spec.json](#)). On retrouve dans ce fichier toutes les spécificités qui font que la blockchain est ce qu'elle est. Nous retrouvons notamment :

- Le nom,
- Le mécanisme de consensus avec ses paramètres
  - o A quelle fréquence un bloc est émis
  - o Qui sont les validateurs
- Le bloc de genèse
- Des paramètres généraux : prise en compte d'EIP les frais de gaz
- Le soldes de comptes en token natif.

```

{
  "name": "CHAIN_NAME",
  "engine": {
    "ENGINE_NAME": {
      "params": {
        ENGINE_PARAMETERS
      }
    },
    "genesis": {
      "seal": {
        ENGINE_SPECIFIC_GENESIS_SEAL
      },
      "difficulty": "0x20000",
      "gasLimit": "0x2fefdb"
    },
    "params": {
      "networkID": "0x2",
      "maximumExtraDataSize": "0x20",
      "initialGasLimit": "0x1388"
    },
    "accounts": {
      GENESIS_ACCOUNTS
    }
  }
}
  
```

Figure 17. Architecture du fichier `chain-spec.json`

Initialement il n'y a qu'un nœud validateur, émetteur des blocs : c'est le Maître de cérémonie. C'est l'entité centrale de la phase d'initialisation du réseau. Celui-ci doit déployer des contrats intelligents de gouvernance.

Ces contrats intelligents vont permettre de créer

- Une gestion d'accès au réseau
- Un système de vote
- Une Gestion des récompenses pour les validateurs
- Une Gestion des différentes clefs utilisés dans le réseau (Minage/Paiement/Vote)

Le déploiement de ces contrats intelligents modifie la structure initiale du réseau et va permettre de commencer la cérémonie. Cette cérémonie a pour but de distribuer différentes clefs aux futurs acteurs qui vont s'occuper du maintien de la blockchain : les validateurs. Cette gestion des nouvelles clefs et des attributions des rôles se fait par le biais du contrat intelligent **key Manager**

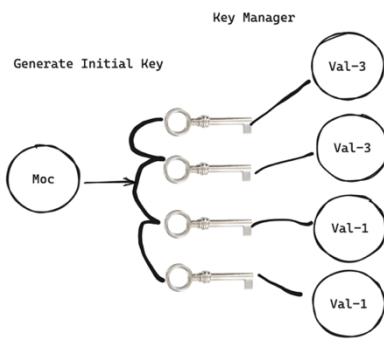


Figure 19. Génération des clefs initiales

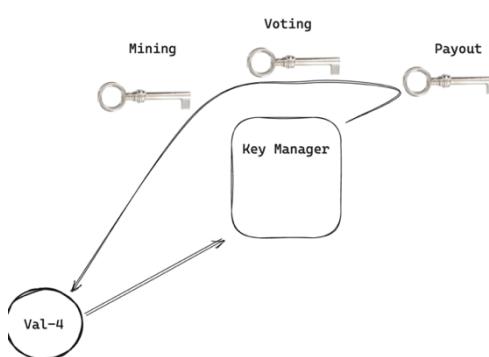


Figure 18. Enregistrement des 3 clefs par le Key-Manager

- 1- Crédit des clefs initiales et distribution aux futurs validateurs
- 2- Chaque validateur vient "s'enregistrer" en donnant sa clef initiale et 3 autres clefs : Minage / Vote / Paiement

Une fois ces clefs générées, le réseau augmente de taille. Il est possible d'ajouter les instances des nouveaux validateurs et de voir la taille du réseau augmenter. Chacun des nœuds validateurs vont participer chacun leur tour à produire et valider les nouveaux blocs.

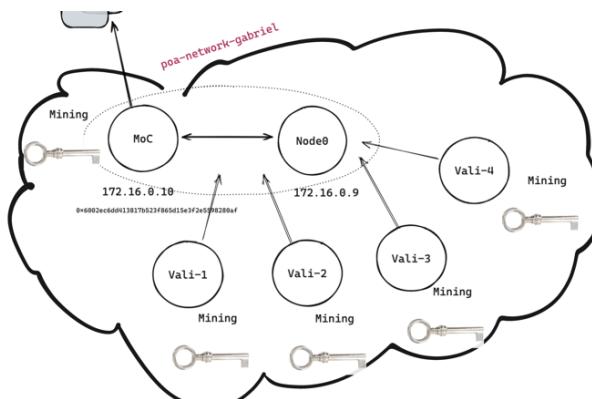


Figure 20. Architecture finale à la fin de la cérémonie

Pour se synchroniser chaque validateur va se connecter aux pairs MoC et Node0 qui sont les deux nœuds d'amorçage

### Test de validations

- Déployer la Dapp : permet la vérification du bon fonctionnement de l'EVM
- Déployer les smarts contracts du PoCo : vérification de la compatibilité de ma chaîne locale avec les produits d'iExec

### Difficultés

Mauvaise architecture pour une image docker, impossibilité de la monter sur un Mac M1 ARM. Pour contourner ce problème, j'ai donc récupéré la logique back-end et adapté celle-ci dans un client node.js à l'aide de la librairie web3Js. Cela est plus efficace, en une seule commande, j'ai pu générer les 3 nouvelles clefs et les transmettre au **Key Manager**.

### Dernières étapes

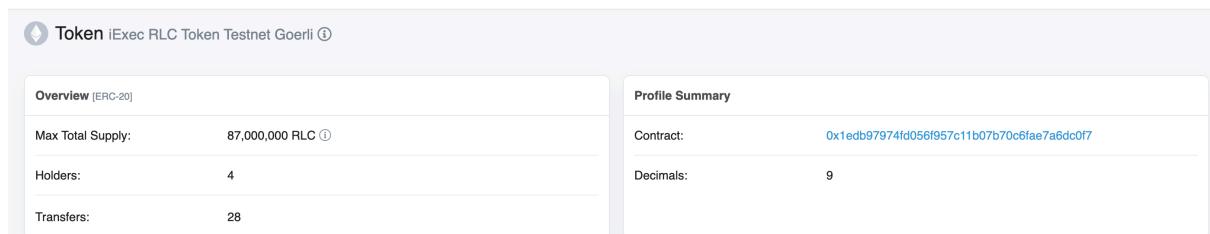
Notre blockchain qui fonctionne de manière locale implémentée actuellement :

- L'algorithme de consensus PoA
- Les contrats intelligents de gouvernance PoA

Il ne manque plus que quelques étapes afin d'avoir une blockchain locale équivalente à Bellecour.

Il faut déployer le jeton numérique d'iExec : le token ERC20 \$RLC. Ce token joue un rôle central dans la pile technologique de l'entreprise. Il a aussi été la monnaie d'échange lors de l'ICO.

Un jeton ERC20, n'est rien autre qu'un contrat intelligent standardisé, il suffit de le déployer à l'aide d'outil de développement



Overview [ERC-20]		Profile Summary	
Max Total Supply:	87,000,000 RLC	Contract:	0x1edb97974fd056f957c11b07b70c6fae7a6dc0f7
Holders:	4	Decimals:	9
Transfers:	28		

Figure 21. Présentation d'un token, présent sur l'explorateur de bloc

Il ne reste plus qu'à déployer le bridge. Ce pont bidirectionnel rend possible le transfert d'asset digitaux d'une blockchain vers une autre. Par exemple, il y a un bridge entre la sidechain Bellecour et Mainnet, et de même pour la sidechain de test Viviani qui est relié à Goerli.

Initialement, il n'y a pas de jetons natifs en circulation sur la blockchain locale et le jeton ERC20 RLC de test n'est déployé que sur Goerli. C'est pourquoi il a fallu déployer un bridge entre le réseau local et le Goerli.

Comment fonctionne un bridge ?

Lorsqu'un utilisateur va vouloir bridge ses jetons de la blockchain A vers la blockchain B, il va envoyer ses fonds au smart contract du bridge A. Un programme tiers (un agent) va observer ces transferts et déclencher le processus : il va communiquer à B que X tokens ont été transférés par l'utilisateur, cela va, soit : libérer des fonds maintenus par le smart contract du bridge côté B, soit le nœuds validateur va recevoir l'instruction de créer des jetons et de les transmettre à l'utilisateur.

Ce déploiement s'effectue donc en deux étapes :

- Déployer les contrats intelligents sur les deux blockchains qui veulent communiquer
- Mettre en place les agents qui vont envoyer les messages entre les blockchains

A la fin de ces étapes il est possible d'envoyer ces jetons RLC depuis la blockchain Goerli vers la blockchain locale. Cela se fait à l'aide d'une Dapp :

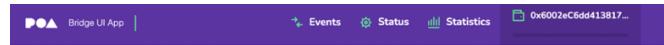


Figure 22. Application web du bridge

Une dernière Dapp est importante pour le bon fonctionnement de la blockchain local : la Gouvernance App. Toute prise de décision concernant la gouvernance de la blockchain doit être soumise à un vote. Chaque nœud validateur du réseau a une clef de vote permettant de participer. On retrouve plusieurs types de proposition :

- Ajout et retrait d'un nœud validateur
- Changement d'adresse d'un smart contract.

Pour qu'une proposition soit appliquée il faut que la majorité ait voté pour.

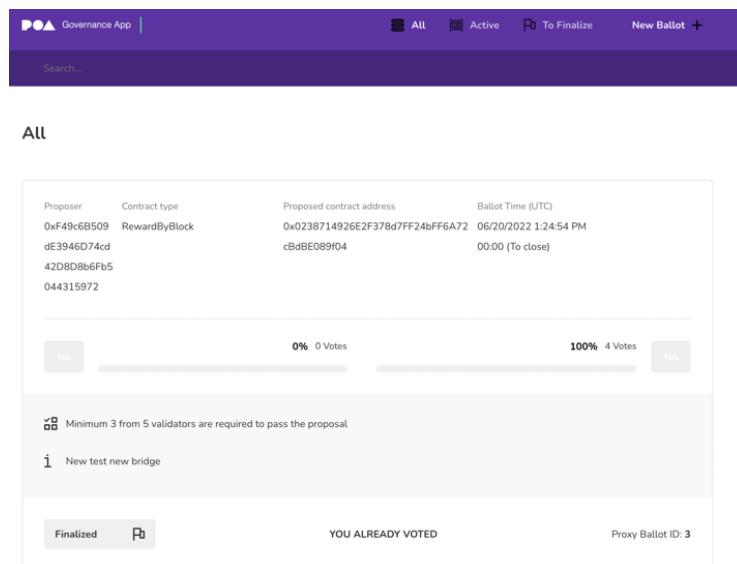


Figure 23. Application web pour la gestion des votes

## Deploying your own chain locally with docker containers

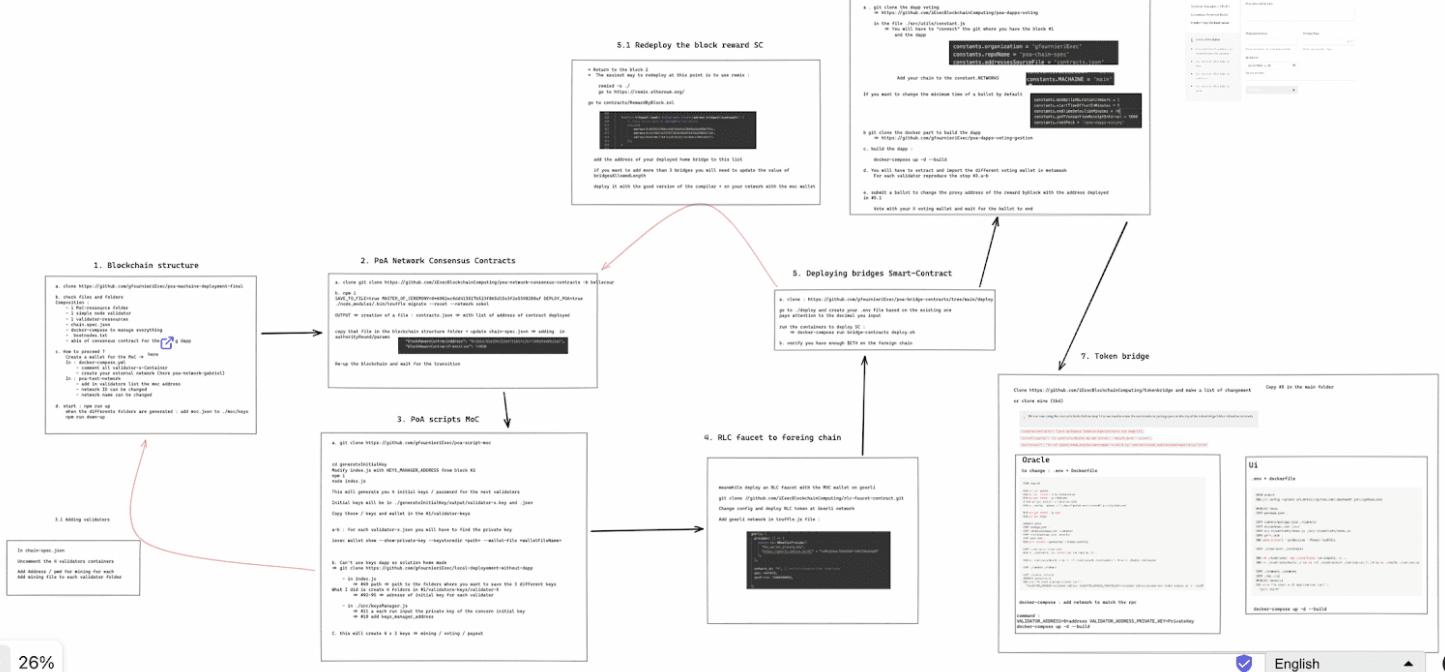


Figure 24. Résumé des étapes à suivre pour le déploiement d'une blockchain locale

## d. Choix du nouveau client et test de migration

La communauté Ethereum maintient plusieurs clients d'exécution open-source : les « clients Ethereum ».

Ceux-ci sont développés par différentes équipes. Cela rend le réseau plus fort et plus diversifié. L'objectif idéal est de parvenir à une diversité sans qu'aucun client ne domine afin de réduire les points de défaillance uniques. La réalité, c'est qu'actuellement 81 % [13] des nœuds font tourner une version spécifique du client Ethereum.

Client	Language	Operating systems	Networks	Sync strategies	State pruning
Geth	Go	Linux Windows macOS	Mainnet, Görli, Rinkeby, Ropsten	Snap, Full	Archive Pruned
Nethermind	C# .NET	Linux Windows macOS	Mainnet, Görli, Ropsten, Rinkeby, and more	Fast, Beam, Archive	Archive Pruned
Besu	Java	Linux Windows macOS	Mainnet, Rinkeby, Ropsten, Görli, and more	Fast, Full	Archive Pruned
Erigon	Go	Linux Windows macOS	Mainnet, Görli, Rinkeby, Ropsten	Full	Archive Pruned
OpenEthereum (Deprecated)	Rust	Linux Windows macOS	Mainnet, Kovan, Ropsten, and more	Warp, Full	

Figure 25. Liste des différents clients Ethereum

Chaque client a ses spécificités, certains vont implémenter certains algorithmes de consensus alors que d'autre non.

Comme expliqué précédemment, le client, OpenEthereum, qui fait pour le moment tourner les blockchains d'iExec est déprécié. Celui-ci n'est plus maintenu par son équipe de développement. Puisque ce domaine évolue rapidement et constamment, de nouvelles EIP sont apportés par la communauté de développeurs, mais ne sont plus forcément supportées par le client. C'est pourquoi il est impératif de changer de client Ethereum.

### *Choix du client*

En réalité, il n'y a que très peu de candidats pour prendre la place de client actuel. Ce qui va contraindre le choix est les algorithmes de consensus que le client implémente ?

Les blockchains d'iExec utilisent la preuve d'autorité (PoA) comme mécanisme de consensus. Ce mécanisme possède lui-même deux versions : Clique et AuRa. Les seuls clients qui implémentent le mécanisme sont : Nethermind et Besu. Mais seul Nethermind utilise la version AuRa de PoA.

C'est donc Nethermind qui pourrait être le client remplaçant d'OpenEthereum. Afin d'être, il faut effectuer des tests vis-à-vis de la technologie d'iExec. Mais pour appuyer ce choix, le projet PoA Network a aussi fait ce choix [14].

### *Tests et observations*

Pour tester si le client Nethermind est fiable, nous devons fournir la preuve qu'il est bien compatible avec les produits d'iExec. J'ai établi plusieurs scénarios permettant de mettre à l'épreuve le client, ils sont faits à partir de ma blockchain de test local.

- Ajouter d'un simple noeud complet Nethermind à notre chaîne
- Prendre un validateur et le forcer à changer de client :
  - o Observer la manière dont le validateur transmet ses blocs et travaille avec les autres.
  - o Éteindre les autres validateurs pendant 10 minutes et observer
- Recréer une blockchain à partir de zéro avec uniquement des validateurs Nethermind et des noeuds complets.
  - o Déployez tous les smart contracts : PoCo, Bridge, PoA consensus, RLC token, etc.
- Tester s'il est possible de traduire la base de données blockchain d'un client OpenEthereum vers Nethermind.

Afin de mettre en place le premier scénario, j'ai dû prendre en main la différence de configurations entre les deux clients. Après avoir compris le fonctionnement de Nethermind, j'ai pu ajouter un fullnode à ma blockchain. À la fin de la synchronisation, le message suivant est apparu :



```
2022-06-28 12:56:31.1075|Rerunning block after reorg or pruning: 24578
(0xc4e2cdbd2dab6a57ee56dd0c3f98020ca5237821327a7f85d1b82f4625765e7c)
2022-06-28 12:56:31.1190|Block from incorrect proposer at block 24578
(0xc4e2cdbd2dab6a57ee56dd0c3f98020ca5237821327a7f85d1b82f4625765e7c), step 331199058 from author
0x6002ec6dd413817b523f865d15e3f2e5598280af.
```

Figure 26. Messages d'erreur de synchronisation

En effet, en observant la blockchain que j'avais mise en place, j'ai pu comprendre que seulement 3 validateurs participaient à la construction du réseau au lieu de 5. J'ai décidé de créer un nouveau

réseau, mais cela peut prendre plusieurs heures. C'est pourquoi j'ai décidé d'automatiser les tâches qui pouvaient l'être au travers de scripts Bash. Cela a permis plusieurs choses.

- Possibilité de créer des blockchains à la chaîne
- Gain de temps dans la création de blockchain à partir de zéro
- Certitude que la blockchain est fonctionnelle

Après avoir contourné ce problème, j'ai pu observer le bon fonctionnement des scénarios 1 et 2. La fin de mon stage se concentrera alors sur la validation des derniers scénarios.

Si les derniers scénarios sont validés, il sera possible à la suite du stage de mettre en place un plan d'action permettant la migration du client Nethermind sur la blockchain de test d'iExec et par la suite la blockchain de production.

#### e. Diagramme de Gantt de mon stage

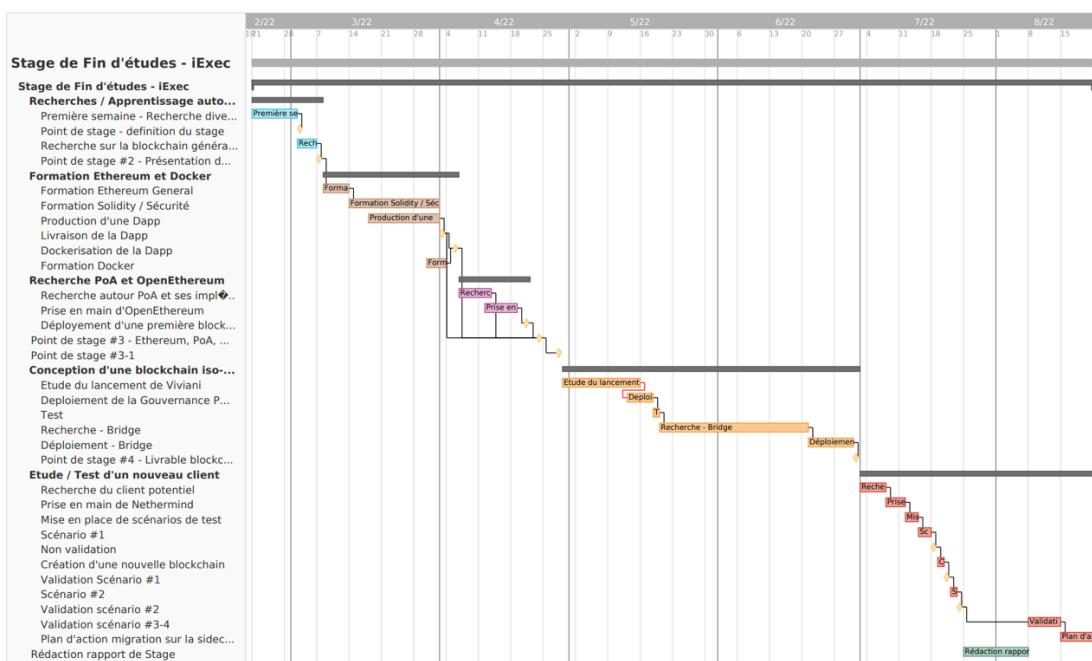


Figure 27. Diagramme de Gantt du stage

## 4. Thèmes SHS

Quand une start-up est sur le point de se lancer, la question du financement de celle-ci est centrale. Avoir une bonne idée sans argent pour la mettre en place ne mène rien, malheureusement. Traditionnellement, cette recherche passe par les fonds propres, mais aussi par l'investissement des capitaux-risques qui sont spécialisés dans l'investissement des jeunes start-up. Avec l'arrivée d'Internet, une nouvelle forme d'investissement a vu le jour : le crowdfunding. Le crowdfunding permet d'ouvrir les portes de l'investissement à quiconque. De la même manière, l'arrivée de la blockchain a permis la création de nouvelles formes d'investissement et de financement auprès des start-up qui veulent se lancer dans la blockchain : les ICO. Par la nature même (pair-à-pair) de la blockchain et la non-régulation, cette forme d'investissement implique énormément de risques pour les investisseurs. Entre 2017 et aout 2018, on peut estimer que les ICO ont levé 28,4 milliards de dollars. Essayons de comprendre ce que sont les ICO et ces implications. Nous verrons ainsi pourquoi les ICO sont une nouvelle forme d'investissement prometteuse, mais aussi risquée. Après avoir décrit

ce que sont les ICO et expliqué l'ICO d'iExec, nous essayerons de comprendre quels risques et avantages, elles impliquent pour les investisseurs et pour les start-up.

### a. Qu'est-ce qu'une ICO ?

L'essor des crypto-monnaies et des blockchains ont donné naissance à une nouvelle forme d'investissement, les ICO (Initial Coin Offerings) [15]. Cette forme de financement permet à une startup de récupérer des fonds très rapidement auprès d'investisseurs du monde entier. Lorsqu'un projet veut lancer une ICO il doit effectuer plusieurs étapes. En s'appuyant de la technologie blockchain il va créer un jeton numérique (une nouvelle cryptomonnaie). Ensuite il va proposer aux utilisateurs de l'acheter en échange de cryptomonnaie. De manière général l'échange se fait avec des cryptomonnaies qui ont une capitalisation beaucoup plus haute, et donc « moins » sujette à la volatilité, tel que le Bitcoin ou l'Ethereum. Contrairement aux autres types d'investissement, une ICO permet à une startup de lever des fonds de manière très rapide et d'avoir la main sur ces fonds instantanément. Alors que les levées de fonds « classiques » peuvent s'établir sur plusieurs années. Une ICO est comparable à une IPO, introduction en bourse, dans laquelle les investisseurs achètent des actions d'une société, mais l'objet échangé n'est pas le même. Avec une IPO on obtient une part de capital d'une entreprise. Alors que souvent le jeton numérique est vu comme un jeton utilitaire permettant d'avoir le droit d'usage pour un futur produit.

La première ICO a eu lieu en 2013, et a été faite pour le financement d'un projet Master Coin, celle-ci a levé 4740 Bitcoin (500k\$ en 2013). La deuxième ICO qu'il est importante de noter est celle d'Ethereum. Si aujourd'hui la blockchain Ethereum est la deuxième blockchain la plus utilisée au monde et que son jeton natif a une capitalisation de marché de 197B \$ le financement du projet s'est fait par ICO, en août 2014. Les acheteurs ont reçu de l'Ether en échange de Bitcoin. Plus de 50 millions d'Ether ont été vendus pour environ 17,3 M \$ avec un prix d'échange de 1 Ether pour 31 centimes \$. Au moment de ces recherches l'Ether à un prix de 1 600 \$.

Avec les chiffres énoncés, on peut déjà remarquer deux choses :

- Pour la startup : procéder à une ICO permet de lever des beaucoup de fonds très rapidement et de plus l'évolution du prix du bitcoin permet de voir sa trésorerie augmenter de façons fulgurantes en un temps très restreint.
- Pour les investisseurs : investir dans un domaine aussi jeune et aussi volatil peut permettre de faire des gains, faciles et rapides.

La création d'Ethereum et des contrats intelligents a permis aux développeurs de créer assez facilement de nouveaux jetons et plates-formes dérivés. Par le biais de ces contrats intelligents il est possible de calculer automatiquement et de distribuer le montant des nouveaux jetons à la fin d'une vente ICO. Entre 2016 et 2018, il y eut une grande bulle spéculative autour des ICO avec une accélération entre mi-2017 et mi-2018 [16].

	2016	2017	2018
Nombre d'ICO	43	453	1082
Total des fonds levés \$	95M181k	6B 576M 372k	21B 576M 147k

Après avoir présenté son projet en août 2016 [17], Gilles Fedack, CEO d'iExec annonce la vente de leur jeton \$RLC en mars 2017, ce jeton permettra l'utilisation du produit d'iExec, le premier cloud décentralisé. Cette vente a eu lieu le 19 avril 2017, avec pour objectif de lever 2 M de \$ au minimum. Il était possible de participer à l'ICO via les blockchains Bitcoin et Ethereum. L'objectif a été surpassé en à peine 3 h. L'ICO a réussi à lever :

- 2 761,761 BTC pour un prix unitaire de 1208,55 \$
- 173 886 ETH pour un prix unitaire de 50,73 \$

Le montant total était de 12M de \$

Avec l'utilisation de la technologie blockchain, tous les comptes sont transparents et public, ainsi chacun peut suivre le ou les comptes (l'adresse) qui possèdent les fonds levés par l'ICO. Par exemple l'adresse principal Ethereum actuelle d'iExec est 0x21346283a31A5AD10Fa64377E77A8900Ac12d469

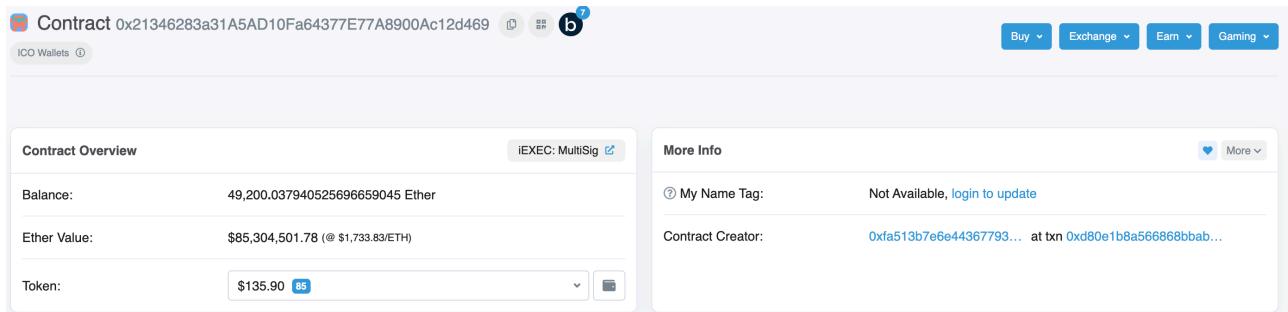


Figure 28. Aperçu du wallet multi-signature d'iExec

Nous pouvons remarquer qu'il y a actuellement 49 200 Ethers sur cette adresse, et que la valeur s'élève à 85 millions de \$.

## b. Quels sont les avantages et les inconvénients de procéder à une ICO ?

Pour répondre à ces questions, il faut savoir de quel côté nous nous penchons, celui du projet, qui effectue l'ICO, ou celui de l'investisseur, qui souhaite participer ? En réalité, il y a des avantages et des inconvénients pour les deux acteurs. Nous allons tout d'abord voir le côté de l'entreprise.

La blockchain n'a pas de frontière, une ICO permet d'avoir des investisseurs du monde entier, de ce fait le public visé est beaucoup plus large. Cette méthode permet de lever des fonds très rapidement : iExec a levé 12 M \$ en moins de 3 h, et d'y avoir accès tout aussi facilement : la start-up possède directement la liquidité issue de l'ICO. Un avantage primordial pour l'entreprise qui veut se lancer dans une ICO est la facilité de monter ce type de financement, beaucoup d'ICO ont profité de la tendance du marché pour effectuer des arnaques ou simplement proposer une ICO sans produire derrière. C'est en réalité l'un des plus gros désavantages pour les investisseurs, car il n'y a aucune régulation qui vient protéger les consommateurs.

Il y a aussi des désavantages, l'un d'entre eux est que contrairement à une campagne de financement classique, où les fonds investis sont en monnaie fiduciaire, les cryptomonnaies sont sujettes à une grande volatilité. Si l'ICO arrive au bon moment, cela peut tout aussi bien être un avantage : les Ethers d'iExec ont été acquis pour un prix moyen de 50 \$ alors que la valeur actuelle est de 1 600 \$. Mais lors de la période d'emballage nombreux sont les projets qui ont levé des fonds et reçus des Bitcoin ou des Ether quelques temps avant le Krach des cryptos de 2018.

Il y a beaucoup d'avantages qui vont pousser un individu à participer à une ICO. La non-réglementation permet à chacun de participer indépendamment du régime politique du pays dans lequel réside l'individu. Elle permet d'une certaine manière de pouvoir déployer des capitaux offrant une couverture contre les chocs politiques et économiques.

Faire partie des premiers investisseurs permet d'avoir accès très tôt, et à prix d'utilisation réduit, pour le futur produit. De plus contrairement aux IPO, les jetons achetés sont beaucoup plus tangibles que les parts de capitaux. Il est important de noter que les jetons achetés sont très volatils et permettent souvent d'avoir une rentabilité des investissements très élevée. Et la transparence de la technologie blockchain permet à chacun de suivre comment est utilisée la trésorerie de la start-up.

D'autre part, la non-régulation permet à chacun de lancer une ICO sans réelle preuve de bonne foi, un KYC n'est pas obligatoire, et généralement une ICO n'est basée que sur un papier blanc présentant

le futur projet et produit. Rien, légalement, n'oblige, cependant le projet a effectivement travailler sur son produit. L'investisseur prend alors des risques en voulant participer à une ICO, il faut presque considérer cela comme un « jeu d'argent » avec des gains conséquents, mais un grand risque. La grande majorité des ICO sont lancées par des entreprises qui sont à un stade très précoce de leur développement. Ces entreprises ont un risque d'échec intrinsèquement élevé. La plupart des jetons qui sont émis n'ont aucune valeur intrinsèque, si ce n'est la possibilité de les utiliser pour accéder à un service ou à un produit qui est en cours de développement par l'émetteur. Il n'y a aucune garantie que les services/produits seront développés avec succès.

En 2018, toute l'attention se tournait vers les ICO, les opportunités de participer à une ICO étaient quotidiennes et chacun participait à cette « ruée vers l'or » [18] [19]. Dans toute cette effervescence, il n'y a eu que très peu d'ICO entièrement légitime. Il semblerait même que 78 % des ICO aient été en réalité des arnaques [20]. La plus grosse arnaque qu'il y a eu, sont les ICO de Pincoin and iFan qui ont été faite par la même société, cette arnaque a touché plus de 32 000 personnes en s'appropriant 660 millions de dollars [21].

### c. Impacts de l'ICO sur iExec

La technologie blockchain a permis à Gilles Fedack de mettre en place son idée de place de marché décentralisé. Le produit d'iExec ne fonctionne que par le biais de son jeton, le RLC. C'est pourquoi, l'idée de levé des fonds par une ICO était naturelle. L'équipe de chercheurs ont annoncé dans leur papier blanc, la roadmap de leur projet qui fera suite à l'ICO en annonçant l'utilisation des fonds de l'ICO pour permettre de construire leur produit.

Cette ICO s'est fait le 19 avril 2017, quelques mois avant le bull-run de 2017-2018 et surtout avant la période d'euphorie autour des ICO. En levant 12 millions de \$ elle s'est hissé comme la 6e meilleure ICO, alors que quelques mois plus tard des ICO ont pu lever plus d'un milliard de \$ [22]. De même, les cryptomonnaies qu'ils ont récupérées ont pris plus de 10 fois leur valeur depuis 2017. « Rien » ne les a obligés à effectivement faire leur produit et le livrer à la communauté, pourtant, ils ont sorti leur produit en trois ans (au lieu de 5).

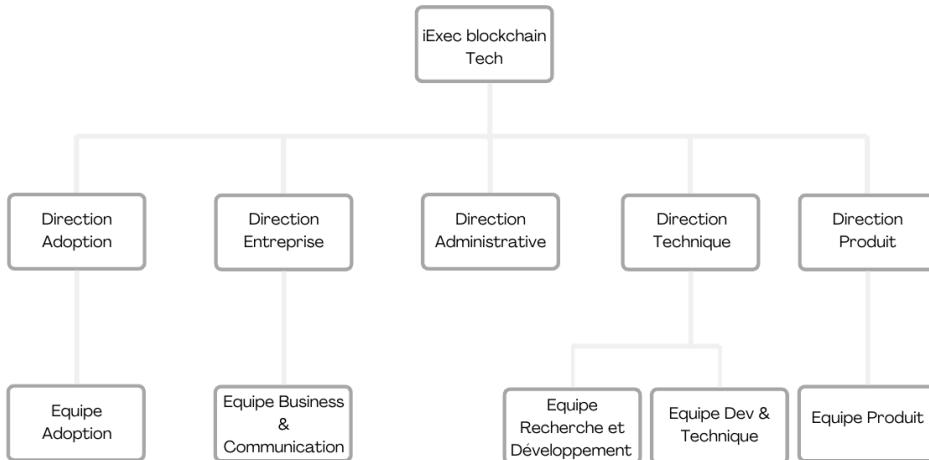
Les détenteurs de jetons peuvent alors utiliser leur plateforme, mais celle-ci ne rapporte pas de chiffre d'affaires à iExec. Pour certains, le fait d'avoir mis en place un jeton donne une position difficile à iExec. Il est facile de comprendre que l'utilisation du jeton par la communauté ne va pas apporter de chiffre d'affaires et que c'est la vente du produit à des entreprises qui va le faire.

iExec cherche de plus en plus à proposer leur solution aux entreprises. Mais généralement, les entreprises se passent du jeton pour utiliser les produits d'iExec, cela dévalorise l'utilisation du RLC, c'est comme s'ils avaient « créés une solution avant même d'avoir trouvé le problème ».

C'est pourquoi ils ont mis en place des incitations pour les projets qui veulent construire par-dessus leur produit. De ce fait, l'entreprise repose actuellement sur la trésorerie acquise lors de l'ICO. Le fait que les investisseurs soient directement une communauté et pas des VC engendre beaucoup moins de pression pour la livraison de produits rentables.

## 5. Métier et projet professionnel

### a. Composition interne et méthodes de management



L'entreprise est divisée en plusieurs équipes, chacune d'entre elle est managée par une direction :

- Adoption : Nelly CORNEJO
- Entreprise : Francis OTSHUDI
- Administrative : Gilles FEDAK et Haiwu HE
- Technique : Oleg Lodygensky
- Produit : Johan MOONEN

L'équipe dans laquelle j'ai effectué mon stage est l'équipe Dev & Technique. Celle-ci se compose de 8 ingénieurs / développeur et de 3 stagiaires actuellement. L'équipe Dev se décompose en différents projets, notamment on peut retrouver les parties Core, Infra, Support, SI, TEE.

iExec a choisi depuis quelque temps d'implémenter la méthodologie Scrum Agile pour la gestion de ses projets. J'ai donc eu la chance moi-même d'appliquer cette méthodologie. Pour permettre cela, plusieurs outils sont déployés au sein d'iExec :

- Confluence : C'est le wiki interne de l'entreprise, il permet de partager, collaborer et d'organiser le travail des équipes
- Jira : Outils de gestions central à la méthode Agile :
  - o Gestion des tickets, du sprint, des stories.

Tout au long de la semaine, différentes réunions sont mises en place pour cadrer la méthodologie Agile. Par exemple, quotidiennement il y a le « daly », elle permet de partager l'avancement de chacun sur les tickets en cours pour le sprint actuel au sein de l'équipe.

A chaque début de sprint, l'équipe choisit des tickets dans le backlog et qui vont constituer le sprint.

A chaque fin de sprint (deux semaines) il y a 3 réunions :

- Sprint Review : présente les avancées de l'équipe Dev et technique aux parties prenantes des projets,
- Sprint rétrospective : permet à l'équipe de faire le point sur le sprint passé et noté les choses à modifier,
- Aperisprint : réunit toutes les équipes d'iExec et permet de partager les résultats de chacun.

Malgré la stratégie de traitement de l'information et d'organisation « bottom-up », la hiérarchie reste très horizontale et la communication avec la direction administrative ne pose pas de problème.

### b. Mon métier d'ingénieur pendant le stage

Lors de ce stage, j'ai pu initialement découvrir le métier d'ingénieur recherche et développement dans le domaine de la blockchain. Mais petit à petit, lors du déroulement de mon stage, je me suis d'abord rapproché du métier de développeur blockchain qui s'occupe notamment de créer d'application full-stack par-dessus la technologie blockchain. Et enfin, la majorité de mon stage s'est penché sur le métier d'ingénieur blockchain, mon tuteur de stage Zied GUESMI exerce lui-même ce poste. Cela m'a permis de comprendre tous les enjeux que représentent l'architecture et le maintien d'une blockchain. Ainsi que le développement de nouvelles fonctionnalités en rapport avec la blockchain qui répondent aux besoins de l'entreprise.

### c. Étape dans mon projet professionnel

Ce stage dans le domaine de la blockchain avait un fort lien avec les cours que j'ai pu suivre lors de mon cursus INSA Lyon Télécommunication. Les bagages informatiques, Devops et gestion de projet étaient fortement utilisés. Ce stage fait suite au premier que j'ai pu faire en entreprise l'année dernière et consolide mes premières expériences en tant qu'ingénieur INSA. Alors que l'année dernière, je n'avais pas d'idée des obligations d'un ingénieur, j'ai pu cette année plus rapidement mettre en place mon travail au sein de l'équipe.

L'environnement n'était pas le même. Lors de ce stage, j'ai pu voir la gestion d'une petite entreprise à taille humaine en pleine croissance. L'environnement de travail chez iExec est très appréciable et je me suis vite habitué aux méthodes de travail mises en place.

À la vue du bilan positif que j'ai pu tirer de ce stage et des opportunités d'embauche au sein d'iExec, c'est pourquoi j'ai postulé pour rejoindre l'équipe Dév & Technique en tant qu'ingénieur Blockchain. Ce poste correspond parfaitement à la continuité de ce que j'ai pu faire lors de mon stage.

## 6. Retour d'expérience personnel

Ces six mois de stage au sein de l'équipe Dev et Technique d'iExec m'ont permis de répondre à beaucoup de questions dont on n'a pas forcément la réponse lors de nos cours à l'INSA.

En effet, bien que mes études m'aient permis d'acquérir une base technique et théorique pour comprendre les bases des métiers d'ingénieurs. Mais le domaine de la blockchain n'est pas forcément un domaine qui nous a été instruit lors du cursus.

La formation nous donne les bases et les prérequis pour nous permettre d'envisager ce domaine. De plus, il y a des cours de spécialisation en 5e année du cursus, dans le développement Ethereum. Mais comme je suis parti en échange Erasmus au premier semestre de cette année, je n'ai pas pu participer à ces cours. La réalité, c'est que j'ai moi-même choisis d'arpenter ce domaine et de me former à l'aide des bases que nous a fournies l'INSA. J'ai pu comparer mes connaissances avec ceux qui ont participé aux cours et comprendre que j'avais aussi appris les notions qui leur avaient été présentées. Le stage m'a conforté dans l'idée de travailler dans le domaine de la blockchain et du Web3.

L'environnement et le domaine dans lequel j'ai évolué m'a rendu plus autonome. Étant donné que le domaine de la blockchain est très jeune, c'est aussi un domaine avec encore peu de ressources concernant les bugs. C'est pourquoi il faut être fort de proposition pour essayer de contourner un problème. Le cursus Télécom de l'INSA nous pousse beaucoup à faire nos propres recherches, mais dans ce stage, il fallait que je pousse mes recherches encore plus loin.

Je pense que les cours de mon département m'ont permis d'acquérir des bagages solides dans la R&D, notamment au travers des différents projets qui nous ont été proposés. Cependant, j'ai compris assez rapidement que les cours ne suffisaient pas, qu'il fallait avoir beaucoup de recul et d'expérience pour avoir des connaissances aussi approfondies que les membres de l'équipe qui m'a entouré.

J'ai toujours apprécié le travail d'équipe, lors de ces derniers mois, j'ai pu travailler de manière générale avec mon tuteur, mais aussi avec toute l'équipe présente dans l'open-space. Pouvoir demander des conseils, des feedbacks était non négligeable au bon déroulement de mon stage.

Ce stage m'a permis de trouver le premier métier que je ferais en sortant de l'INSA. Cela m'a donné un premier aperçu de la vie au sein d'une startup évoluant dans un domaine aussi jeune qu'intéressant que la blockchain. J'ai pu comprendre qu'il ne fallait pas abandonner et savoir se faire confiance même si parfois les résultats n'arrivent qu'au bout d'un certain temps.

## 7. Conclusion générale

Pour conclure, je peux affirmer que ce stage au sein de l'équipe Technique d'iExec m'a permis de découvrir le monde professionnel dans ce domaine particulier qui est la blockchain. Je considère cette expérience comme une réussite, autant d'un point de vue personnel que professionnel et relationnel en entreprise. La taille de l'entreprise m'a permis une bonne et rapide intégration auprès de toutes les équipes. Plus particulièrement, j'ai eu de la chance de me retrouver intégrée à une équipe sympathique qui a su m'accueillir chaleureusement et me mettre à l'aise rapidement. J'ai pu monter en compétences à différentes échelles et j'ai beaucoup appris.

Je pense avoir su répondre aux attentes de l'équipe et que l'objectif du stage a été atteint. Maintenant, que le nouveau client a été sélectionné, il faut mettre en place la migration de celui-ci, d'abord sur la blockchain de test et ensuite sur la blockchain de production.

## Table des sigles et des abréviations

**BTC:** Bitcoin

**B2B:** Business to Business

**CTF:** Catch the Flag

**EIP:** Ethereum Improvement Proposals

**ETH:** Ethereum

**EVM:** Ethereum Virtual Machine

**ICO:** Initial Coin Offering

**IPO:** Initial Public Offering

**PoCo:** Proof of Contribution

## Bibliographie

[1] Documentation d'OpenEthereum. **OpenEthereum.** Récupéré sur <https://openethereum.github.io/> (consulté le X.X2022)

[2] Gnosis. **Gnosis client development team Joins Erigon (formerly Turbo-Geth) to Release Next-Gen Ethereum Client.** Sur : Médium. Disponible sur : <https://medium.com/openethereum/gnosis-joins-erigon-formerly-turbo-geth-to-release-next-gen-ethereum-client-c6708dd06dd> (consulté le X.X2022)

[3] Adam Hayes. **What Is a Blockchain?** Sur: investopedia. Disponible sur <https://www.investopedia.com/terms/b/blockchain.asp> (consulté le X.X2022)

[4] Satoshi Nakamoto. **Bitcoin: A Peer-to-Peer Electronic Cash System.** 2008. Disponible sur <https://bitcoin.org/bitcoin.pdf> (consulté le X.X2022)

[5] Dr. Gavin Wood. **ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER.** 2013- Aujourd'hui. Disponible sur : <https://ethereum.github.io/yellowpaper/paper.pdf> (consulté le X.X2022)

[6] Radar Relay Inc. **Ethereum Gas Explained** [en ligne]. Disponible sur : <https://ethgas.io/> (consulté le X.X2022)

[7] Oliver Jumpertz. **The Ultimate Smart Contract Developer Roadmap: From Zero to Hero** [en ligne]. Disponible sur : <https://blog.oliverjumpertz.dev/the-ultimate-smart-contract-developer-roadmap> (consulté le X.X2022)

[8] Loom Network. **Learn to Code Blockchain DApps By Building Simple Games** [en ligne]. Disponible sur: <https://cryptozombies.io/> (consulté le X.X2022)

[9] Rekt. **RONIN NETWORK – REKT.** Sur rekt.news. Disponible sur : <https://rekt.news/ronin-rekt/> (consulté le X.X2022)

[10] Openzeppelin. **The Ethernaut** [en ligne]. Disponible sur : <https://ethernaut.openzeppelin.com/> (consulté le X.X2022)

[11] ConsenSys Software Inc. **Sweet Tools for Smart Contracts** [en ligne]. Disponible sur: <https://trufflesuite.com/> (consulté le X.X2022)

[12] Nomic Foundation. **Ethereum development environment for professionals** [en ligne]. Disponible sur : <https://hardhat.org/> (consulté le X.X2022)

[13] Ether alpha. **Diversify Now Improve Ethereum's resilience by using a minority client** [en ligne]. Disponible sur: <https://clientdiversity.org/> (consulté le X.X2022)

[14] Varasev. Switch from OpenEthereum to Nethermind on Sokol. Sur Forum PoA Network. Disponible sur :<https://forum.poa.network/t/switch-from-openethereum-to-nethermind-on-sokol/6528> (consulté le X.X2022)

[15] The European Securities and Markets Authority. **ESMA alerts investors to the high risks of Initial Coin Offerings (ICOs).** ESMA50-157-829 [en ligne]. 2017. Disponible sur : [https://www.esma.europa.eu/sites/default/files/library/esma50-157-829\\_ico\\_statement\\_investors.pdf](https://www.esma.europa.eu/sites/default/files/library/esma50-157-829_ico_statement_investors.pdf) (consulté le X.X2022)

[16] Bitni. **Statistics for cryptocurrency, ICO, IEO and STO** [en ligne]. Disponible sur : <https://bitni.com/site/coin-schedule/stats> (consulté le X.X2022)

[17] Gilles Fedak. **Liste des Article de Gilles Fedak.** Sur Médium. Disponible sur : <https://medium.com/@gilles.fedak> (consulté le X.X2022)

[18] Zetzsche, Buckley, Arner, Föhr. **The ICO Gold Rush: it's a scam, it's a bubble, it's a super challenge for regulators** [en ligne]. 2018, University of New South Wales Law Research Series. Disponible sur : <https://deliverypdf.ssrn.com/delivery.php?ID=463070022024114098069086072072095109057049057076086029076124073089067073006026120093117033048052107045040093004030097024000102021041003015023084117097075098127027057034084067078067115070114094080023124090093068070123007029089030100102077019107029101&EXT=pdf&INDEX=TRUE>

[19] Lana Swartz. **Theorizing the 2017 blockchain ICO bubble as a network scam** [en ligne]. 2022 Vol. 24(7) 1695–1713. Disponible sur : [https://llaannaa.com/preprint\\_swartz\\_nms\\_ico.pdf](https://llaannaa.com/preprint_swartz_nms_ico.pdf)

[20] Sherwin Dowlat. **CRYPTOASSET MARKET COVERAGE INITIATION: NETWORK CREATION.** 2018. Disponible sur : [https://research.bloomberg.com/pub/res/d28giW28tf6G7T\\_Wr77aU0gDgFQ](https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ)

[21] William Suberg. **Vietnam: Pincoin, Ifan ICOs Exposed As Scams That Allegedly Stole \$660 Million.** Sur Cointelegraph. Disponible sur : <https://cointelegraph.com/news/vietnam-pincoin-ifan-icos-exposed-as-scams-that-allegedly-stole-660-million>

[22] Elementus. **The ICO market is not collapsing. It's maturing** [en ligne]. Disponible sur : <https://elementus.io/blog/ico-market-august-2018/>