Quelques applications des blockchains pour l'Espace

Jérôme Lacan

jerome.lacan@isae-supaero.fr

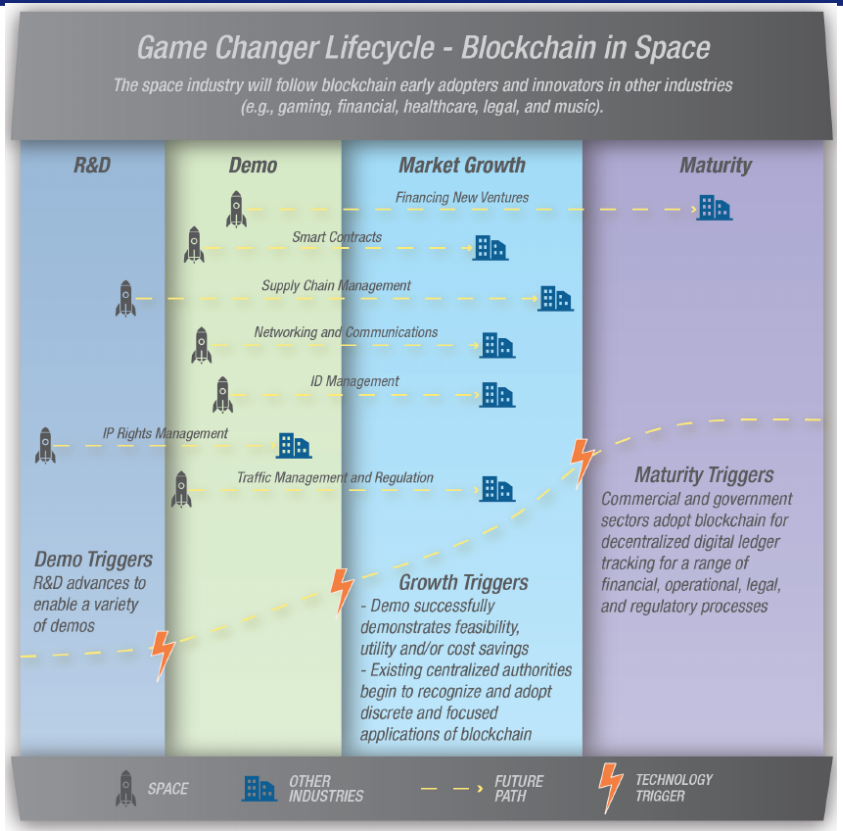
isae
Institut Supérieur de l'Aéronautique et de l'Espace
SUPAERO

Plan de la présentation

- Partie I : Applications des blockchains à l'Espace
  - Entreprises/Startups/Fondations
  - Agences spatiales
- Partie II : Travaux à l'ISAE sur cette thématique
  - présentation de l'équipe
  - Gestion des débris spatiaux sur une blockchain
  - des essaims de drônes vers les essaims de satellite

Résumé des intérêts des blockchains

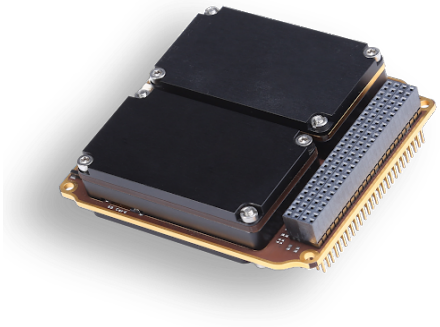
- Remplacer des autorités centralisées
- Propriétés : transparence, efficacité, privacy et gestion des accès, Résilience, ….
- Applications potentielles dans le secteur spatial :
  - Financement et gestion d'entités distribuées
  - Supply chains, gestion de la PI,.

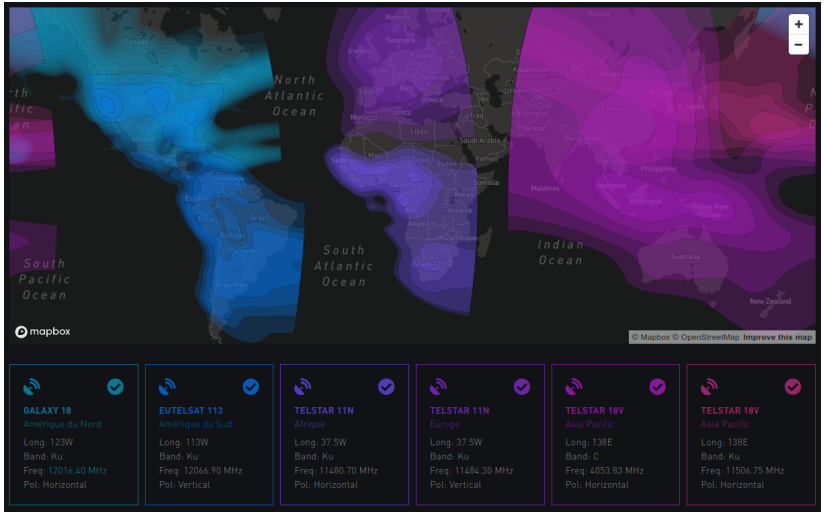


[Blockchain In The Space Sector, Karen L. Jones, 2020

Entreprises/Startups/Fondations (1)

- **SpaceChain** :
  - Intégration de satellites dans des réseaux de blockchains ; comme le propose la société SpaceChain.
  - 1er satellite lancé en jan. 2018 (nœud Qtum sur Raspberry Pi). Noeud blockchain embarqué sur l'ISS en dec. 2019 avec un OS dédié (nœud Etehreum)
  - Objectif de création d'une communauté
  - CTO : Jeff Gardzik
- **Blockstream** : diffusion des mises à jour de Bitcoin par satellite sur 5 satellites géo-stationaires, autres grosses contributions (Liquid network) . Directeur général : Adam Back



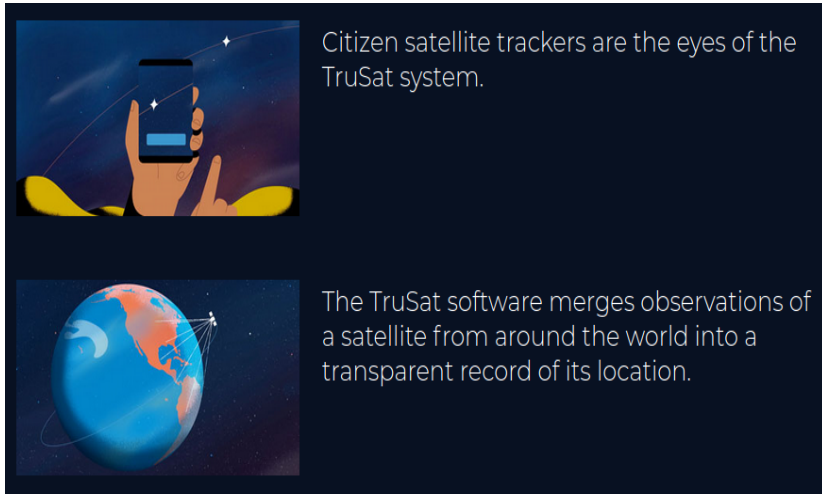


Entreprises/Startups/Fondations (2)

- **SpaceBit** : favoriser l'innovation liée aux technologies blockchains pour l'espace.

- Consensys Space : **Trusat** - géolocalisations de débris spatiaux stockés sur une blockchain

- **EtherSat** : développement de standards de communication sol-espace.

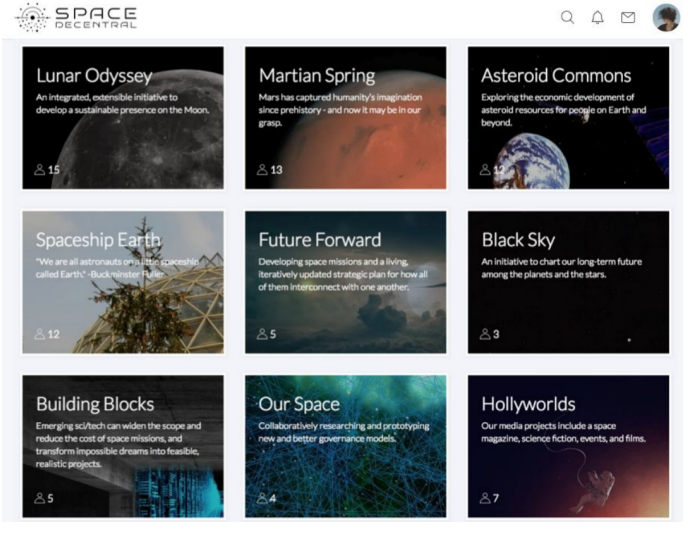


Entreprises/Startups/Fondations (3)

- Localisation : XYO Foundation

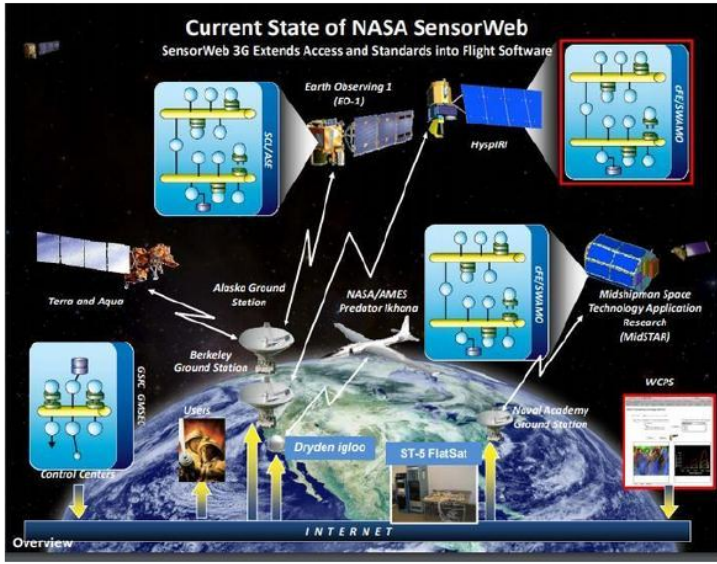
- Space Impulse : Communauté autour l'Espace : place de marché B2B sur une blockchain pour réduire les délais et les couts de mise en orbite (d'accès à l'espace).

- Space Decentral :
  - Principal objectif : A Decentralized Autonomous Space Agency
  - Travaux actuels dans le cadre de la startup Autark : gouvernance distribuée, coopérative numériques, ...



Agences spatiales

- NASA :
  - SensorWeb : réseau de capteurs partageant des données
  - financement : RNCP: A Resilient Networking and Computing Paradigm for NASA Space Exploration, 2017-2020, 300k$



- ESA :
  - Space 4.0 – interconnection d'acteurs du spatial facilitant les échanges (administratifs, financiers, ...).
  - collaboration spaceChain

- DLR, JAXA, ... : peu de résultats visibles
  -

Partie II : Activités Blockchain à l'ISAE-SUPEARO

BLEND group : BLockchains for aEronautical aND space systems

https://websites.isae-supaero.fr/blockchain/blockchains-at-isae-supaero

Activités de Recherche

- Chercheurs permanents impliqués : Caroline Chanel, Corentin Chauffaut, Jonathan Detchart, Thibault Gateau, Jérôme Lacan
- Doctorants :
  - Doriane Pérard (ISAE) - Blockchain scalability analysis
  - Marina Dehez Clementi (ISAE-ENAC-Macquarie University)) - Blockchain-enabled Trust and Security in Distributed Systems (2018-)
  - Lucas Gicquel (CIFRE - Edokial) - Optimisation des blockchains de consortium (2019-)
- Plateforme :

Résultats

Publications

- Perard, D., Lacan, J., Bachy, Y., & Detchart, J. (2018). Erasure code-based low storage blockchain node. Blockchain 2018 (Halifax, Canada), July 2018.
- Dehez-Clementi, M. and Larrieu N. and Lochin E. and Kaafar D. and Asghar H.. When air traffic management meets blockchain technology : a blockchain-based concept for securing the sharing of flight data. IEEE/AIAA 38th Digital Avionics Systems Conference (DASC), Sept. 2019
- Pérard D. , Gicquel L., Lacan J. , "BLOCKHOUSE : Blockchain-based distributed storehouse system", 9th Latin-American Symposium on Dependable Computing (LADC), November 2019
- M. G. Santos De Campos, P. E. U. de Souza, C. P. C. Chanel and J. Lacan Blockchain-Based Multi-UAV Surveillance System, Second Symposium on Blockchain for Robotics and AI Systems, Dec. 2019
- Dehez-Clementi M., Deneuville J. C., Lacan J., Asghar H. and Kaafar D., Who let the DOGS out: a Group Signature scheme with Distributed Opening for Auditable but Anonymous 4th International Workshop on. Cryptocurrencies and Blockchain Technology - CBT sept. 2020. Abstract video link: https://youtu.be/7ITWAZizs5Y , Full video link : https://youtu.be/RjSboWYeRnw

Projets étudiants (passés)

Reverse-engineering the Ethereum Geth client to implement back-end attacks on Blockchain, J. Yates, A. Stum, June 2017

Reliable messaging dapp : email-like system on Ethereum - P. Courgeon, E. Puydebois, C. Gil, september 2017

Ethereum evaluation with Blockbench integration, I. Dahan, June 2018

Transparent call for tender dapp, on Ethereum, P.L. Saint, June 2018

Benchmark Hyperledger Fabric vs Quorum - L. Gicquel, November 2018

Erasure Coding integration in Geth, X. Goffin, June 2019

Comp'Chain : **Delivey and certification of skills**, based on Quorum, B. Allard, L. Sterlin and V. M. Leguet, collaboration with with Bruno Ilponse and Laurent Dairaine,

Blockchain-Based Multi-UAV Surveillance System, based on IOTA, Mario G. Santos de Campos,

Study of the **IOTA** blockchain and its Fast Probabilistic Consensus algorithm, A. Vandewalle, June 2020

Distributed Ledger for **Depreciating Space Tracking Data**, C. Dahdah, C. van Leeuwen, Z. Kheil, June 2020

Distributed Ledger for Depreciating Space Tracking Data

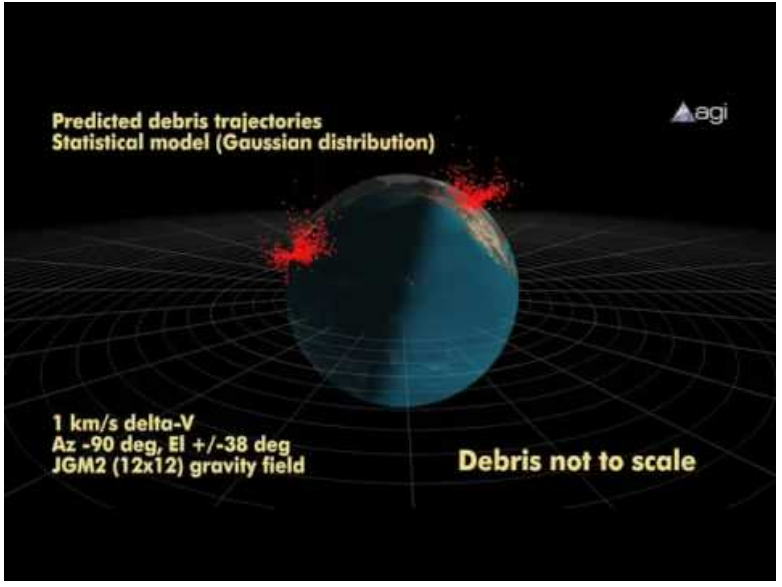
Authors : C. Dahdah, C. van Leeuwen, Z. Kheil, J. Detchart, T. Gateau, J. Lacan

Contexte : localisation des débris spatiaux

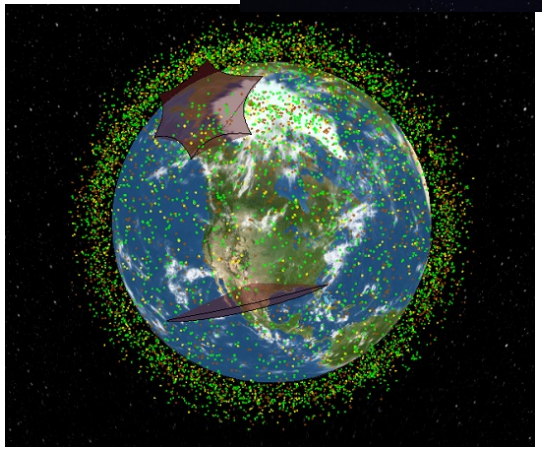
Problème : Syndrome de Kessler

Examples :

- Feb. 2009 - Iridium 33 vs Kosmos 2251
- Sept. 2019 : Aeolus vs Starlink 44



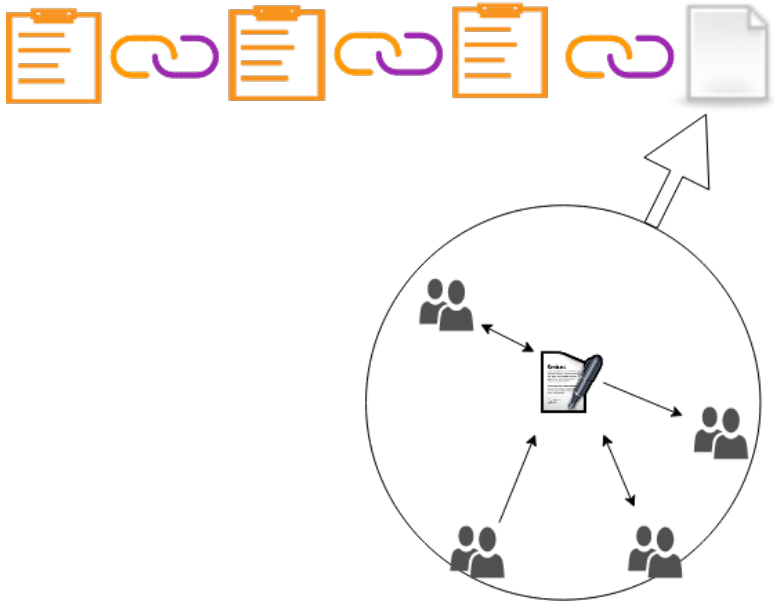
Privatisation de ce marché



Comment améliorer la transparence et le partage de ces informations ?

Utilisation d'une **blockchain**

- accessible
- immuable
- consensus

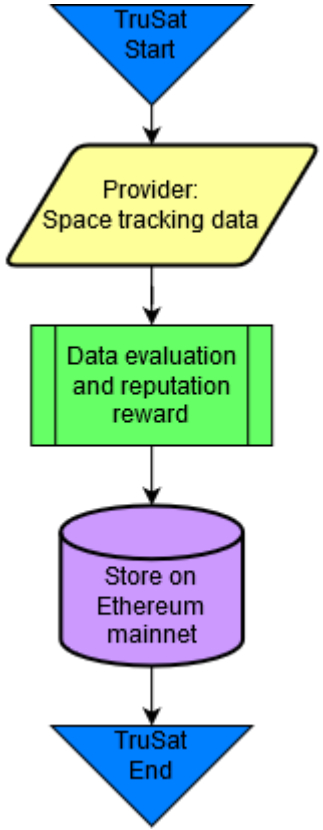


et TRUSAT ?

mais TRUSAT l'a fait !

son modèle ⇒

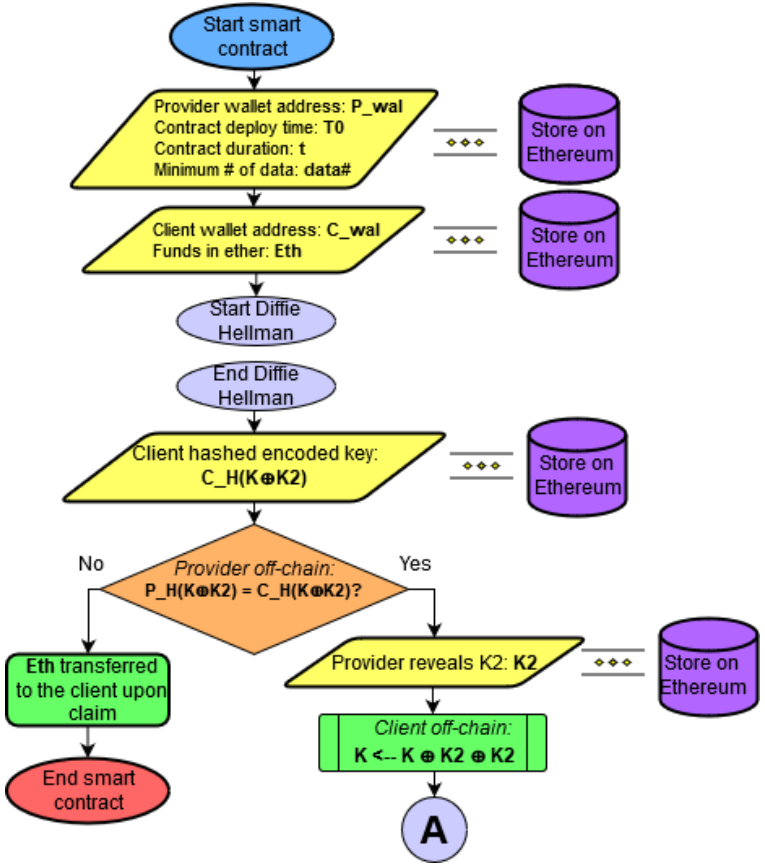
problème : et tous les nouveaux acteurs commerciaux ?!?



Notre proposition pour intégrer des acteurs commerciaux

Principe :

1) un utilisateur **chiffre** ses observations et les **stocke** sur la blockchain
2) un autre utilisateur intéressé **achète la clé de déchiffrement**
3) la **valeur** des données **décroit** avec le temps
4) la **clé** est finalement publiée après un certain temps

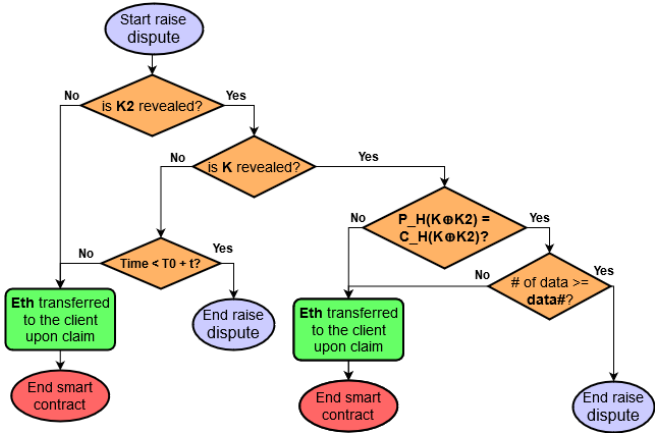


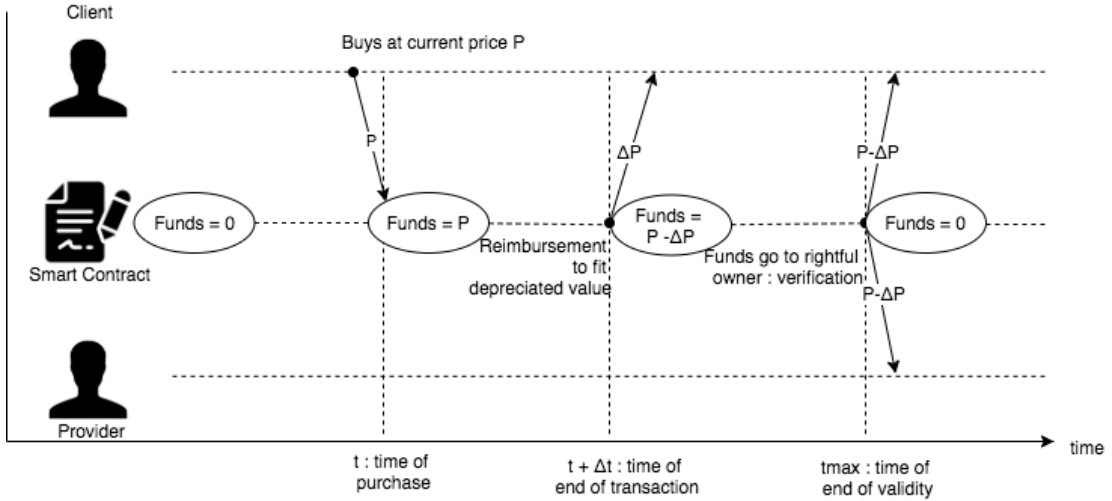
Définition de protocoles utilisant la blockchain comme intermédiaire

Principe :

1) le protocole cryptographique gère la variation de la valeur de la donnée

2) la transparence de la blockchain permet au smart contract de trancher en cas de dispute





Implémentation complète de la solution

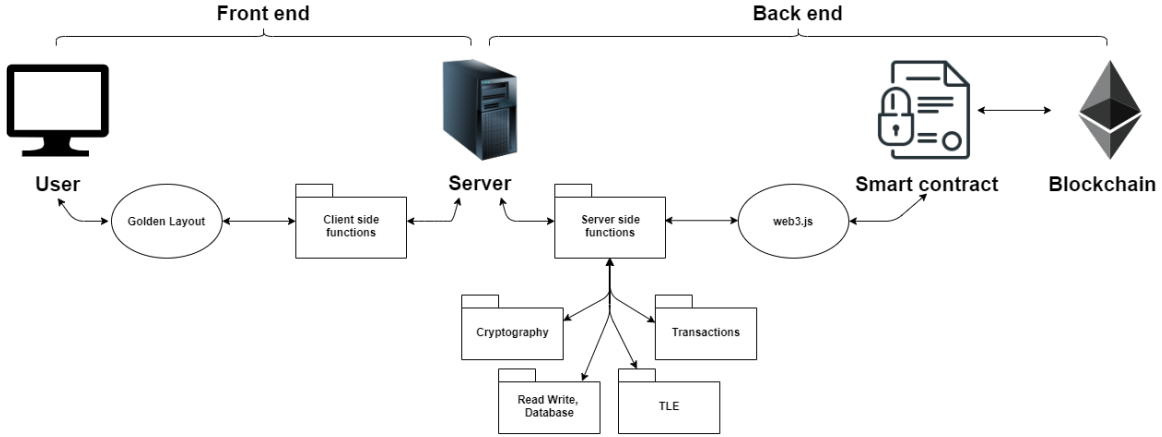
Blockchain : Ethereum

Client : Besu

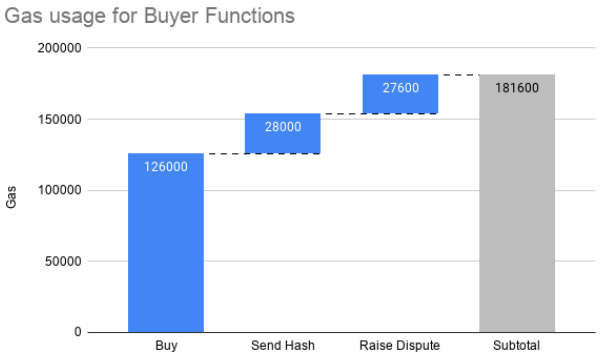
Smart contracts : solidity

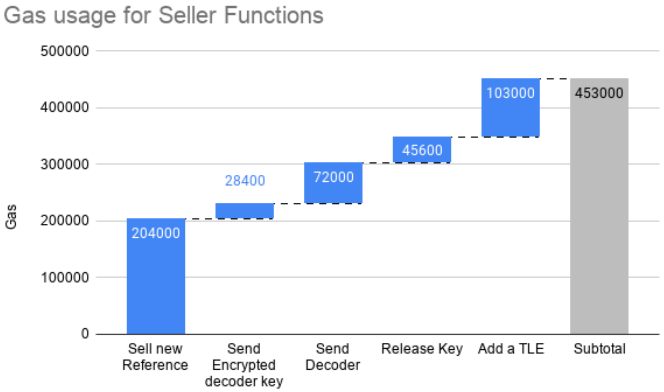
Serveur : nodeJS

Interface web : javascript

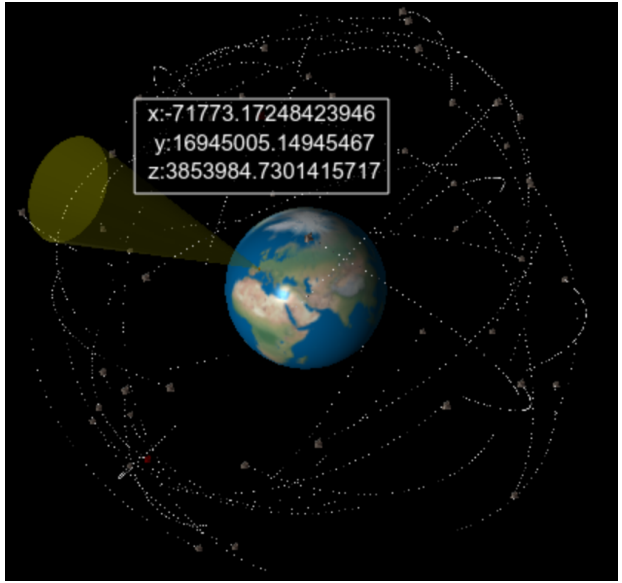


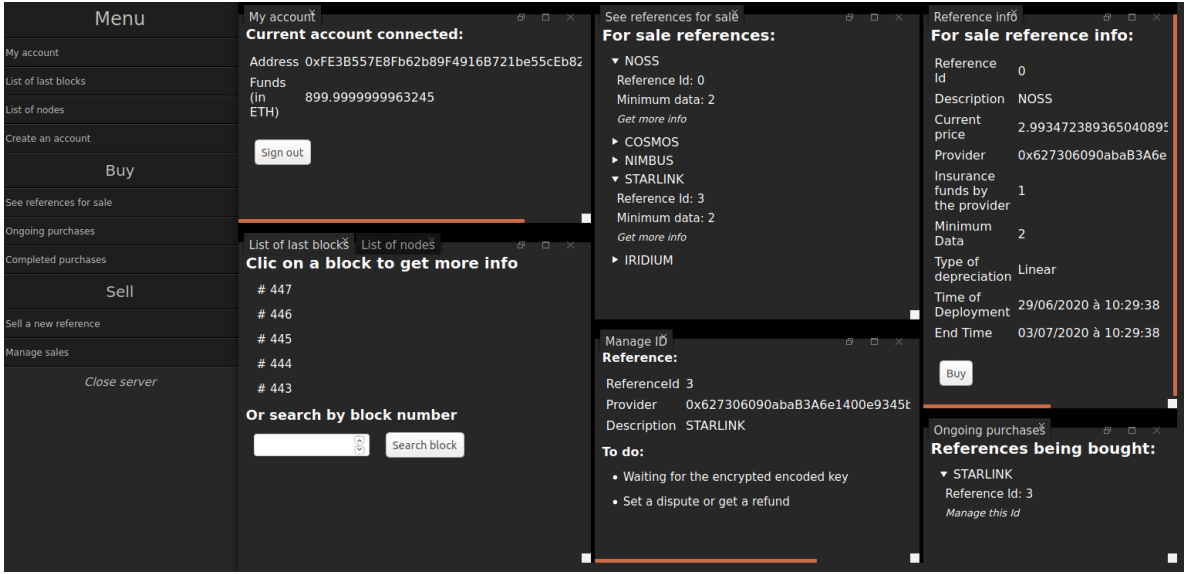
Analyse des couts :





Démonstration en cours de construction





+ soumission pour publication

Autre travail en cours : Blockchain-Based Multi-UAV Surveillance System

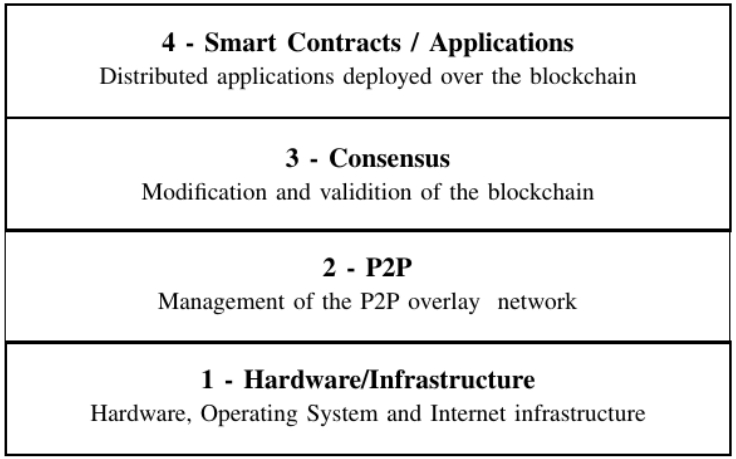
- Auteurs : Mario G. Santos de Campos, Caroline Chanel, Corentin Chauffaut, Jérôme Lacan

- Point de départ : Bitcoin est probablement le système le plus **résilient** au monde

- Objectif : montrer que cette résilience peut s'appliquer dans d'autres contextes : **réseau de drônes autonome**

- Application au scénario d'un système de surveillance par un essaim de drônes

- Des drones et/ou des PoI peuvent être **défaillants/malveillants**



Scénario

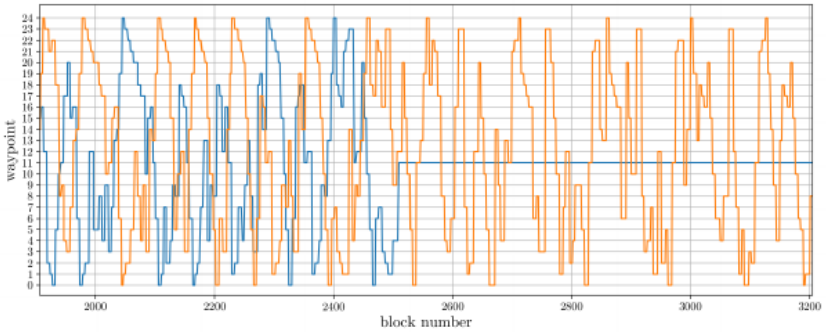
- Un essaim de drones doit surveiller un certains nombre de Point d'Intérets (PoI)
- Ces drones peuvent être « loués » par leur propriétaire au système contre rémunération pour le travail accompli
- Des PoI se rajoutent et se retirent du système dynamiquement. Ils paient le service au système.
- La blockchain doit :
  - gérer tous ces échanges financiers
  - assurer une répartition des mission optimales : visites régulières mais non prévisibles de chaque PoI, rémunérations homogènes des drônes
  - gérer les utilisateurs défaillants/malveillants ainsi que la dynamique du contexte.
-

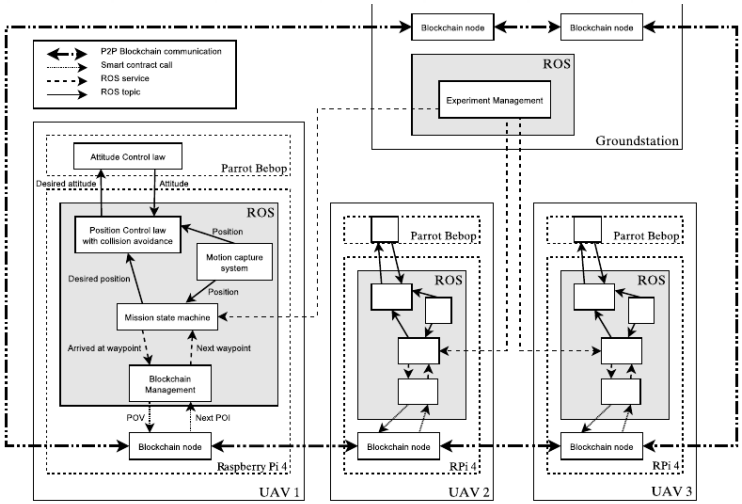
Résultats

- Smart contracts de gestion des différents utilisateurs
- Algorithme d'Intelligence artificielle (basé su la théorie des jeux) implementé dans un smart contract pour l'allocation des tâches
- validation des résultats
- Implémentation sur des drônes embarquant des nœuds blockchain Ethereum

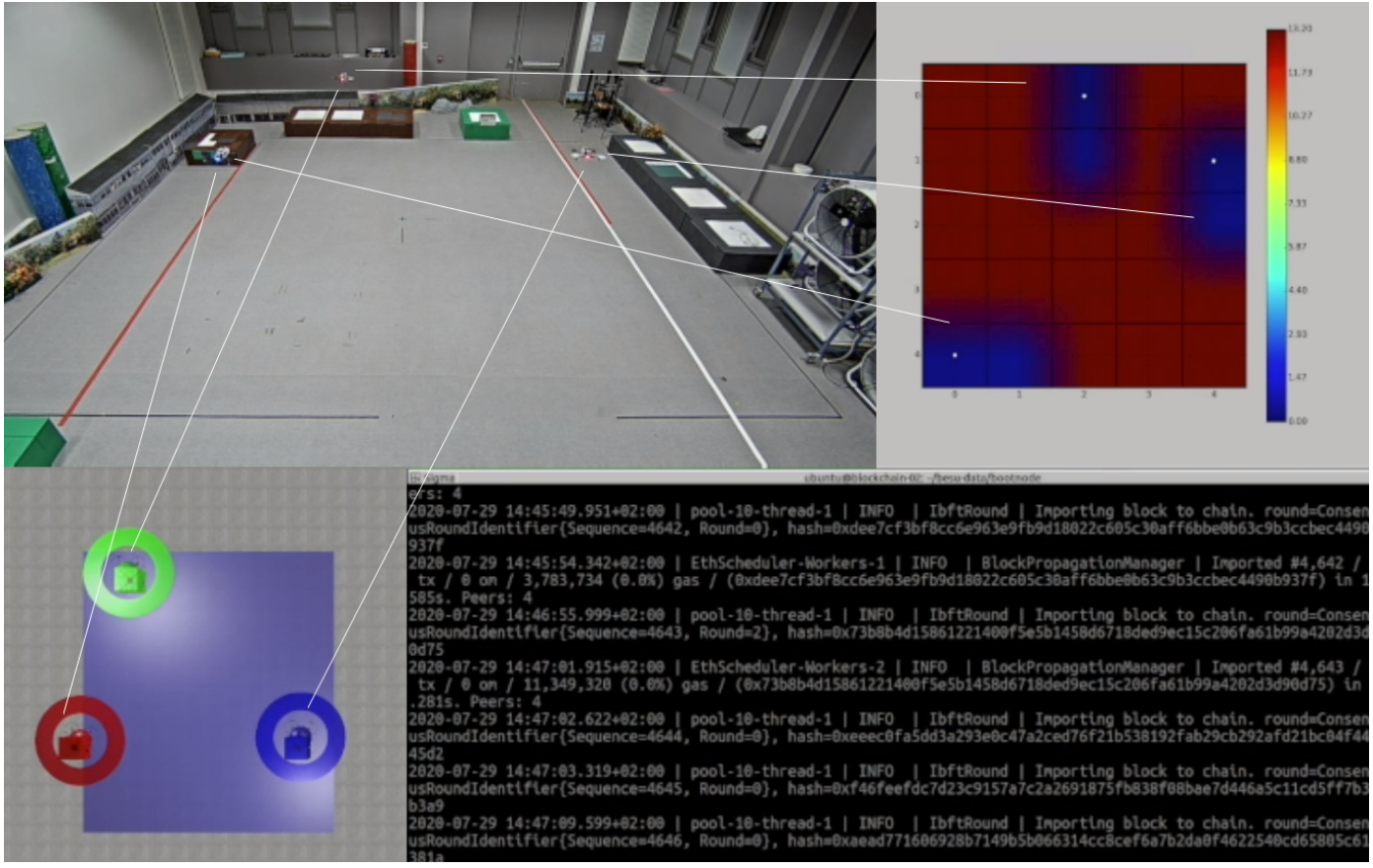
publications en cours

-





Démonstration



Version spatiale ?

- **Objectif spatial** : application aux **essaims de satellites**
  - intérêt de résilience évident
  - excellent compromis « autonomie / contrôle du système »
  - challenges en terme d'implémentation
-

Conclusions

1) Applications spatiales des blockchains :

- applications classiques à toutes les industries (supply chains, places de marché automatisées, …)
- ouverture du secteur spatial à de petits acteurs
- potentiel intéressant pour des essaims de satellites

1)Questions ?