Blockchain Principles

Aerospace Applications

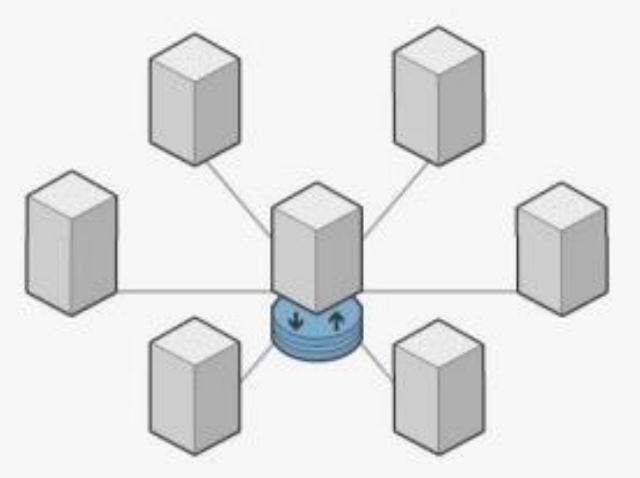
Jérôme LACAN

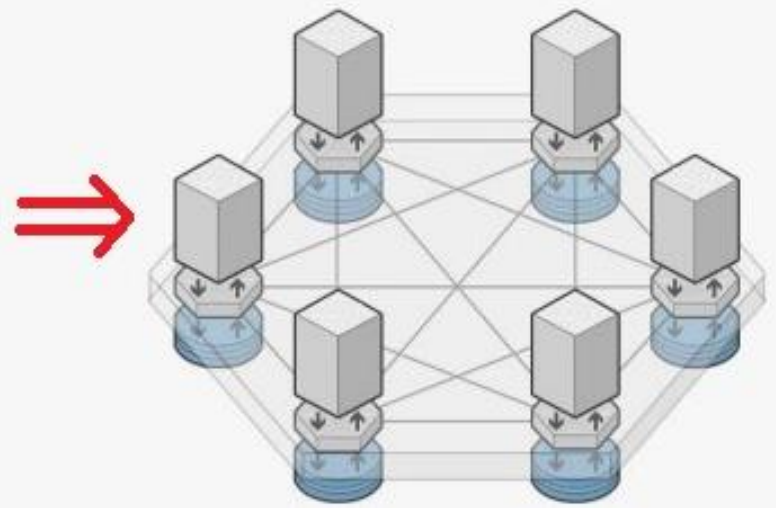
30/11/2023

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

Blockchain

- C’est un système qui permet de passer d’un système de ce type à celui-ci :





- Une blockchain est un système de gestion et de stockage de données distribué :
  - sans organe de décision central
  - immuable

A quoi peut servir une blockchain ?

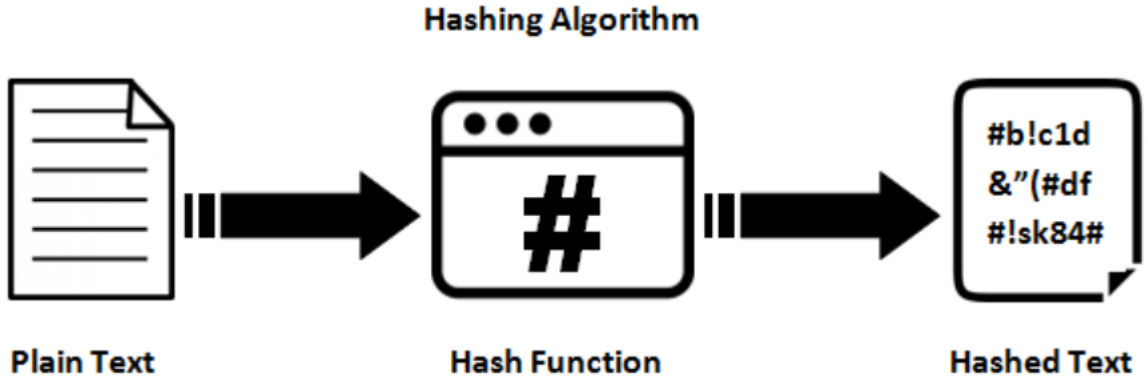
- système de gestion d'une crypto-monnaie : Bitcoin ...
- système assurant la "transparence"
- système de certification de documents
  - cadastre (Ghana), tout document notarial
  - certification de diplômes/compétences
- système informatique impliquant plusieurs entités ne se faisant pas confiance
- A terme, système informatique remplaçant tout intermédiaire sans valeur ajoutée...

Eléments techniques : fonctions de hachage

- **Fonction de hachage** H : crée une empreinte numérique de taille fixe (ex : 256 bits) d'un document

- Propriétés de H :
  - **Résistant aux collisions** : ∀x, il est "difficile" de trouver y tel que H(y) = x
  - **faible complexité**

- Principales fonctions de hachage : SHA-256, SHA-512, SHA-3



Eléments techniques : signature

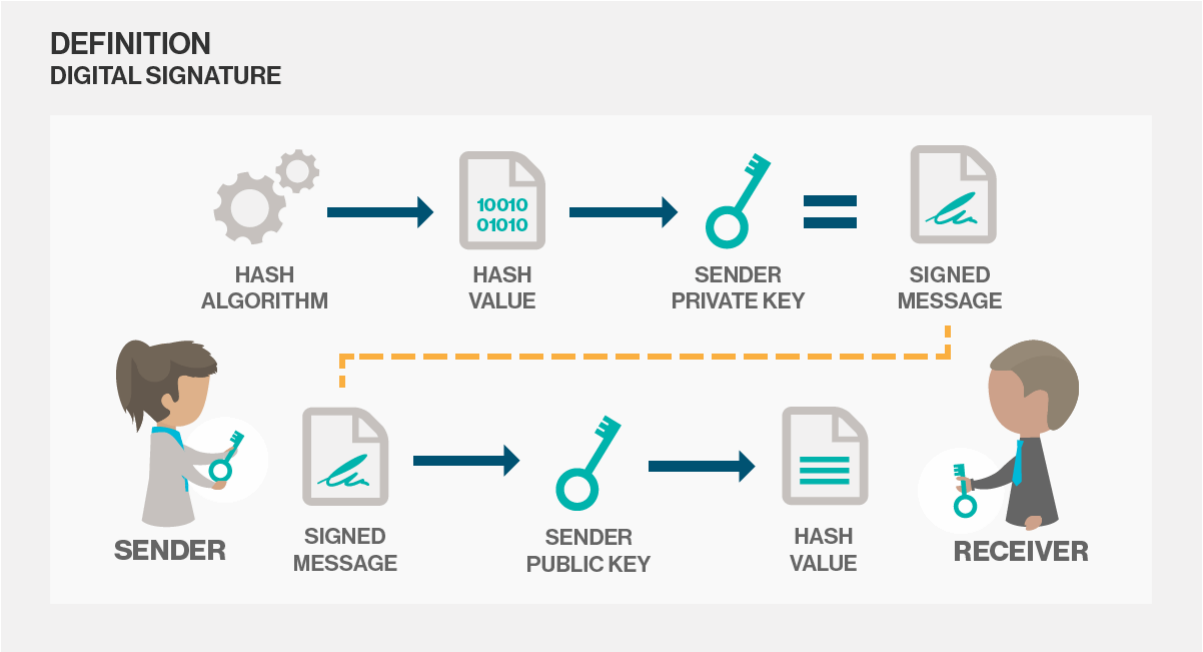
- Pour qu'une personne puisse signer électroniquement un document,

elle doit générer un couple de clés :

  - une clé **privée**, accessible uniquement à la personne qui veut signer
  - une clé **publique**, accessible à tous

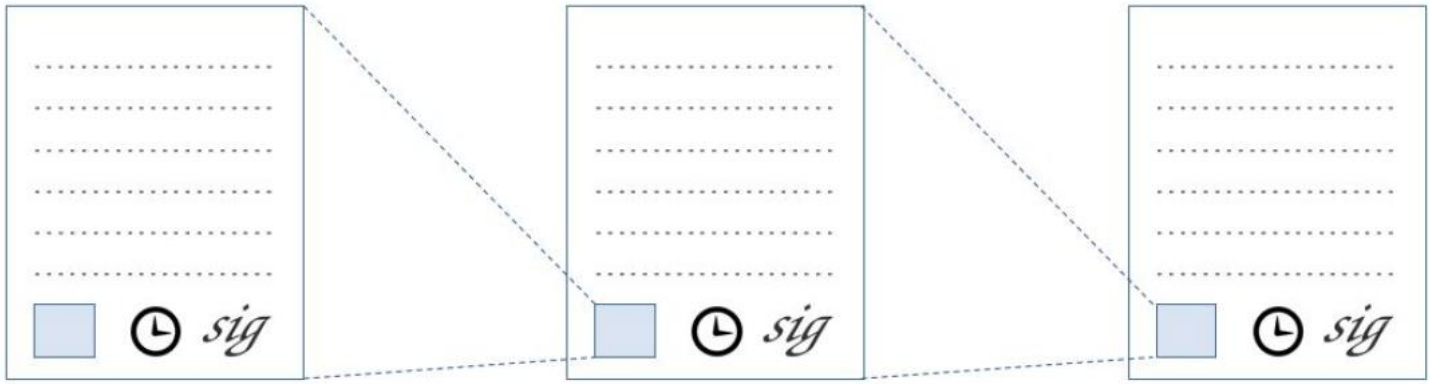
- En pratique, l'utilisateur crée une "signature" à partir d'un document avec sa clé privée. Tout le monde peut vérifier avec la clé publique que la signature correspond bien au document.

- Fonctionnalité inverse du chiffrement.



Eléments techniques : Chaîne d'horodatage

- Principe de la chaîne d'horodatage : liaison de documents par des hashs.



- Chaque nouveau bloc ajouté à la chaîne contient le document, la date à laquelle il a été généré, le hash du bloc précédent et la signature de cet ensemble d'éléments.

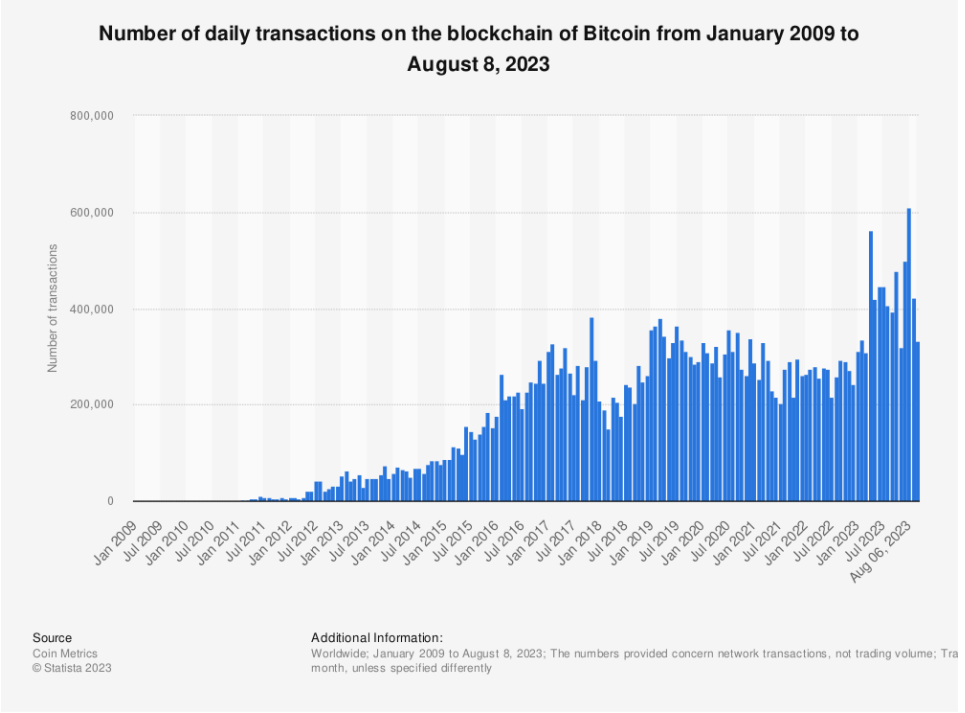
- Chaque nouveau bloc valide ainsi tous les blocs précédents !

Eléments techniques : dépense énergétique basée sur la résolution de problèmes

- Le but est de s'assurer qu'une entité a "payé" quelque chose pour obtenir un résultat ,
- On définit un problème mathématique qu'on ne peut résoudre qu'en dépensant une certaine d´epense d'´energie.
- Introduit pour résoudre le problème des spams d'email. Appliqué ensuite aux cryptomonnaies.

Bitcoin

- Organisation et implémentation de ces briques de base pour construire un système de crypto-monnaie fiable et complètement décentralisé.
- Novembre 2008 : ”bitcoin : A Peer-to-Peer Electronic Cash System” par Satoshi Nakamoto
- Janvier 2009 : première version open-source du code et premiers blocs
- Depuis, succès croissant...



Bitcoin : principes généraux

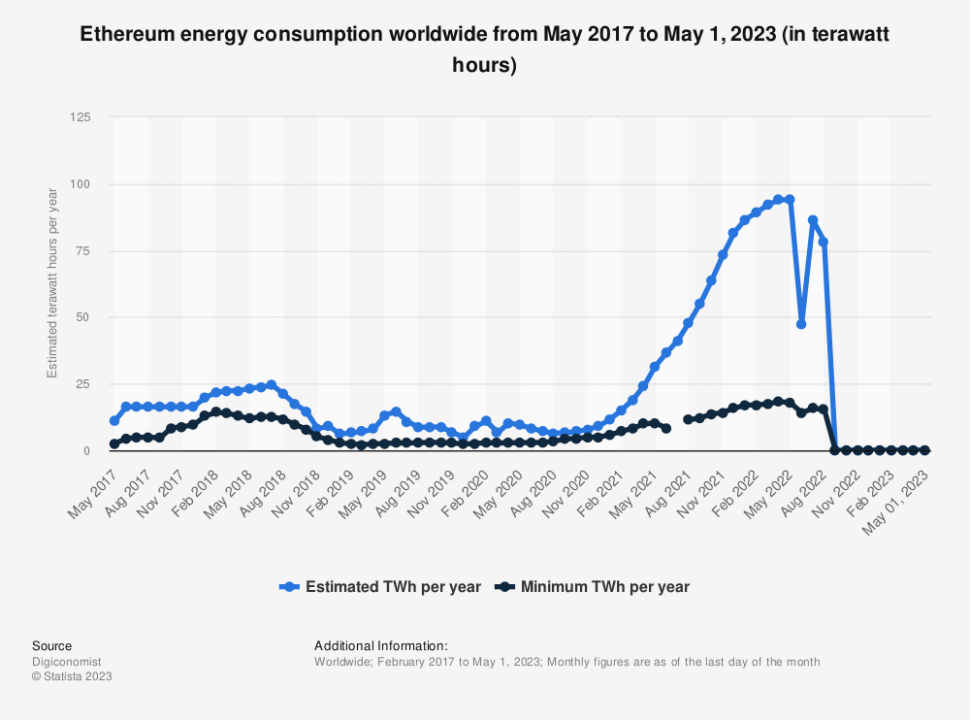
- toutes les transactions du système sont stockées dans la blockchain
- la blockchain (~ 529.60 GB) est répliquée sur tous les nœuds du réseau (> 10000)
- chaque utilisateur est identifié dans le réseau par sa clé publique et ne peut interagir avec le réseau qu'avec sa clé privée.
- le système stocke uniquement des transactions (et pas le solde des comptes)
- utilisation d'un consensus de type "preuve de travail" (proof of work) qui résout le problème de la double dépense.

Bitcoin : consensus

- les transactions souhaitées sont diffusées à tous les nœuds du réseau
- chaque nœud vérifie les transactions proposées et construit un bloc avec les transactions valides et le hash du bloc précédent
- il mine ce bloc : il cherche un nonce tel que le hash soit inférieur à un seuil
- toutes les 10 minutes (en moyenne), un nœud réussit à trouver un bon nonce et diffuse le bloc et son nonce à tous les autres nœuds qui l'ajoutent à leur blockchain.
- le nœud qui a trouvé le nonce reçoit une récompense (constituée de nouveaux Bitcoins et de pourboires)

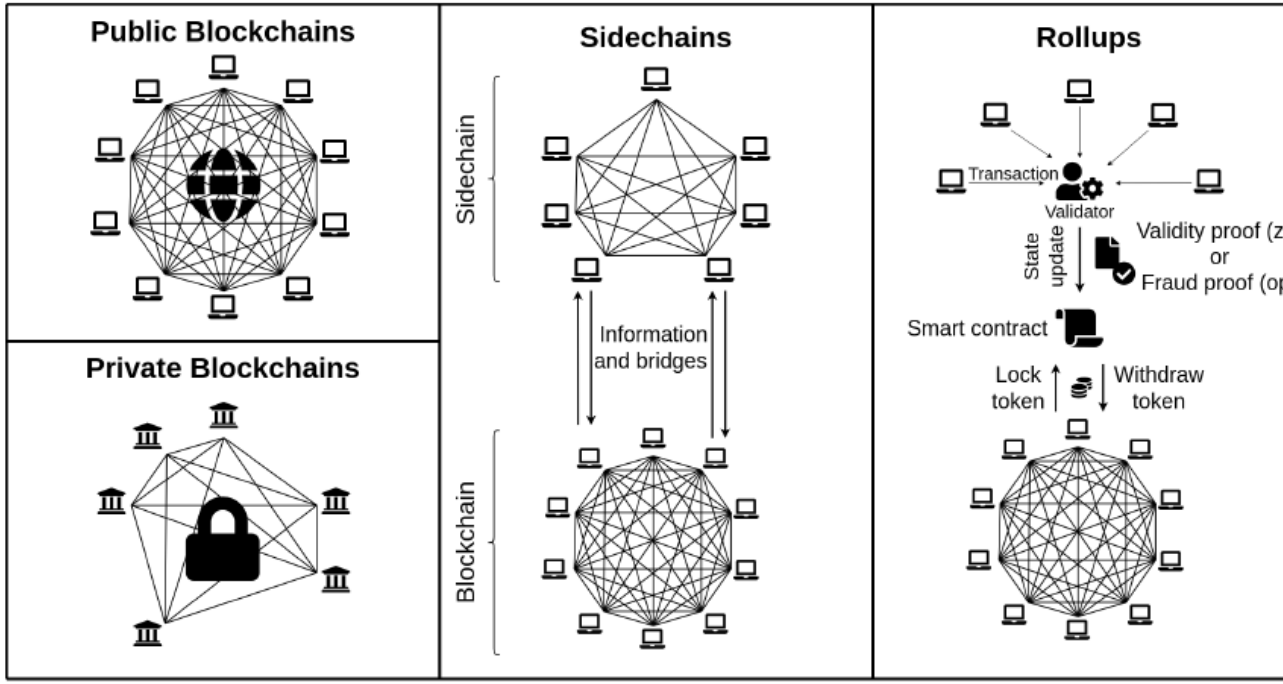
Autres blockchains : Ethereum – smart contracts

- Ethereum développe les Smart Contracts :
  - Smart Contract : programme s'exécutant dans une machine virtuelle (Turing-complete) de la blockchain.
  - utilise un principe de compte plutôt que de UXTOs
- Hard-fork en juillet 2016 suite à un bug dans un smart contract de The DAO
- Consensus basé sur la preuve d'enjeu (proof-of-stake) depuis novembre 2022
- Implémentations disponibles en versions publique et privée



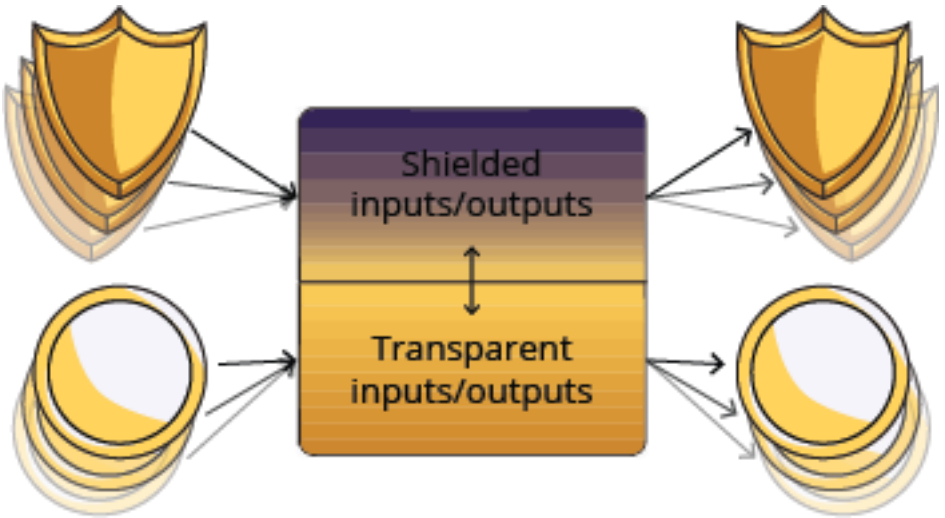
Autres blockchains : Ethereum – layer 2

- Le futur d'Ethereum s'écrit avec les « layers 2 »
  - sidechains
  - Rollups : espace hors de la blockchain qui va stocker des preuves de ses activités sur la blockchain
- 2 techniques principales pour les rollups :
  - rollups "classiques" : basés sur les fraud proofs
  - zk-rollups : basés sur les preuves à divulgation nulle (zero knowledge - zk-proofs)



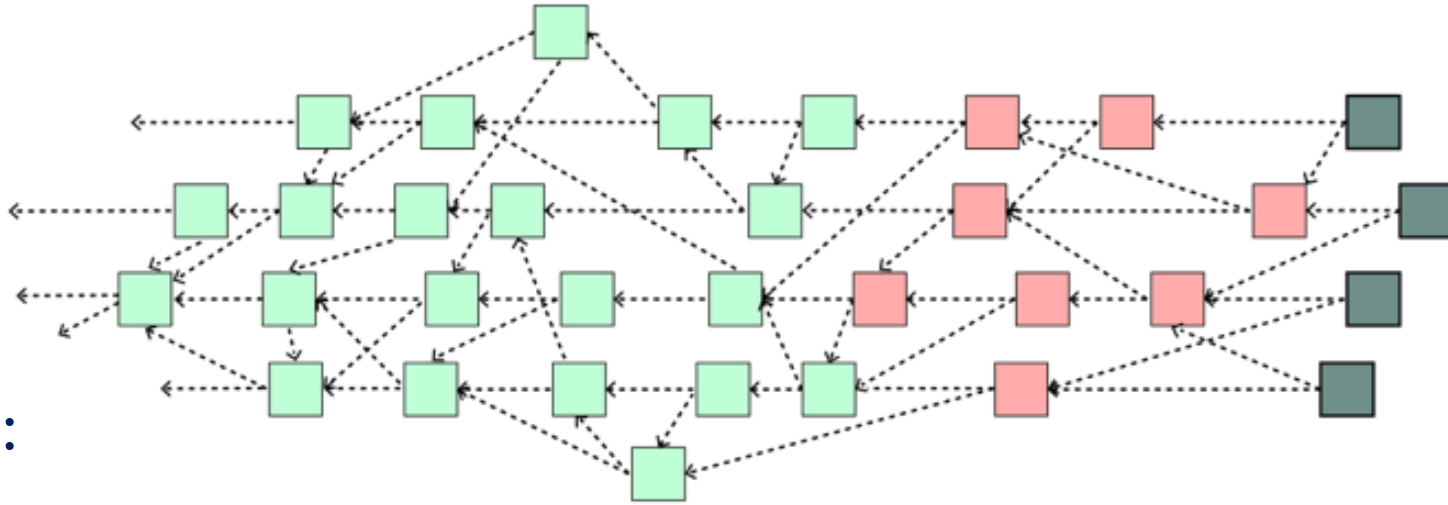
Nouveaux concepts : anonymisation

- Monero : anonymat basé sur des anneaux de signatures et sur les adresses furtives
- Zcash :
  - permet de cacher le montant et l'identité des personnes impliquées dans une transaction
  - basé sur des preuves sans divulgation d'information (Zero-knowledge)



Autres blockchains

- Ripple
  - blockchain privée portée par la société Ripple depuis 2012
  - succès important : concurrent du système bancaire SWIFT
- Solana
- Avalanche
- nouvelles générations - ex. IOTA :



Aerospace applications

- Aerospace markets
- Collaborative observation :
  - Space observation
  - Sky observation
- Decentralized management of networks of mobile nodes
  - Drones
    - Surveillance systems
    - Data delivery
  - satellites

blockchain @ ISAE

Staff :

Caroline Chanel
Marina Dehez-Clémenti
Jonathan Detchart
Thibault Gateau
Corentin Chauffaut
JL
...

Students :

Thomas Lavaur
Deborah Conforto Nedelmann
Antoine Stevan
…

Thématiques de recherche :

Applications aérospatiales des blockchains
Rollups
Preuves zero-knowledge
Cryptographie distribuée
implémentations
…

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

Aerospace applications

- Aerospace markets
- Collaborative observation :
  - Space observation
  - Sky observation
- Decentralized management of networks of mobile nodes
  - Drones
    - Surveillance systems
    - Data delivery
  - satellites

A1

A2

A3

A4

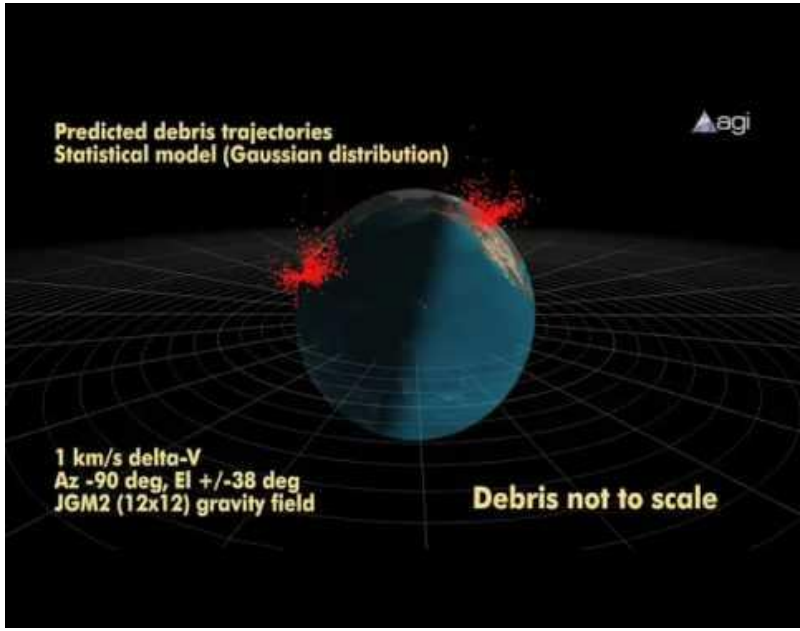
A5

A1 : Distributed Ledger for Space Tracking Data

Context : localization of space objects (including debris)

Problem : no global database

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

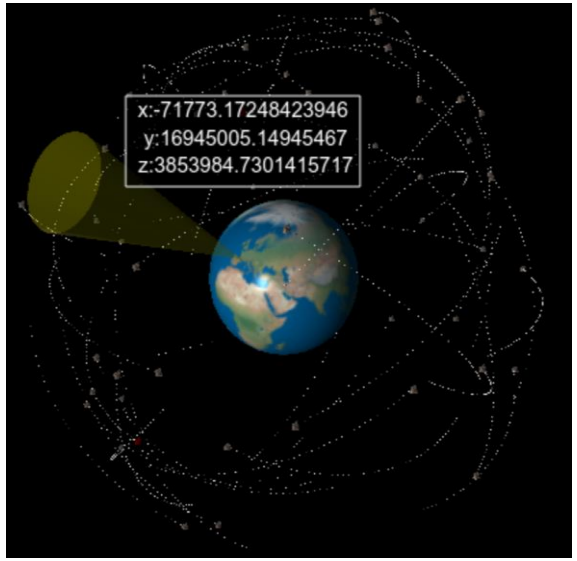


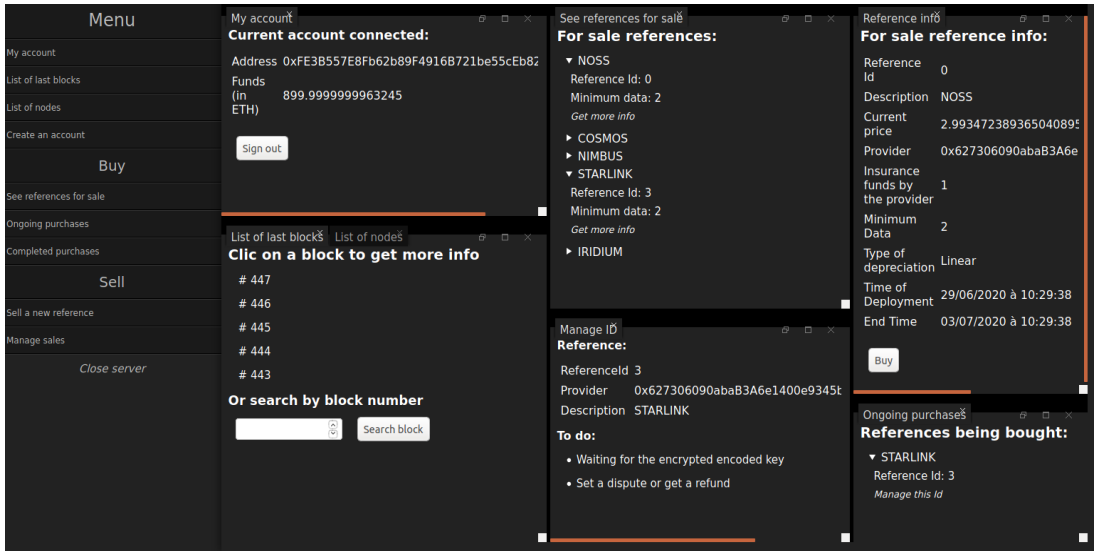
CNES R&T (with starting blocks)
Definition of a blockchain application building a market of space objects
Providers propose « measures data » of space obkects
Clients buy these measures to define the objects orbits

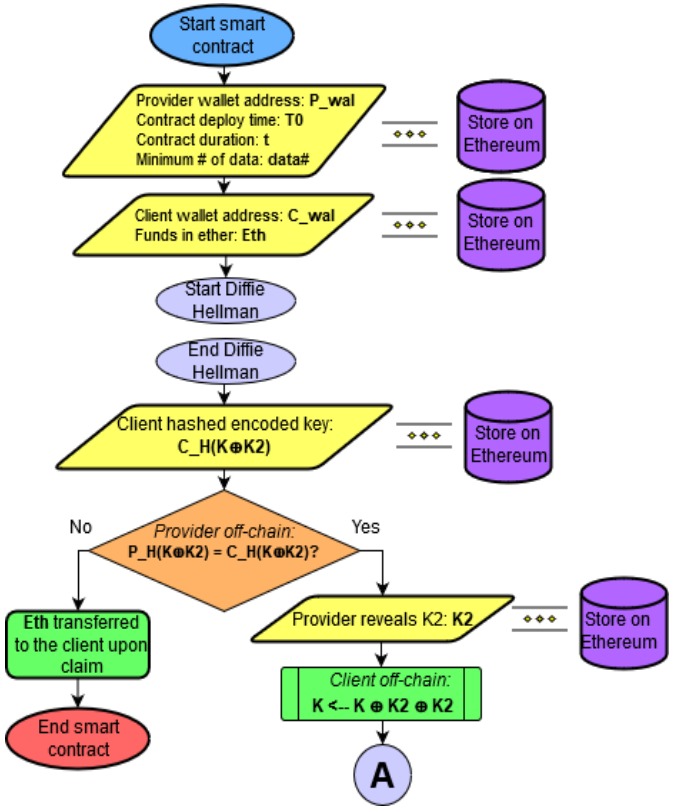
A1.bis : Distributed Ledger for Depreciating Space Tracking Data

Additional work : definition of a protocol to exchange data with depreciating price. Full implementation in solidity

[Dahdah, C., Van Leeuwen, C., Kheil, Z., Lacan, J., Detchart, J., & Gateau, T. (2021). Enabling Monetization of Depreciating Data on Blockchains. 7th International Conference on Information Systems Security and Privacy (ICISSP 2021)]



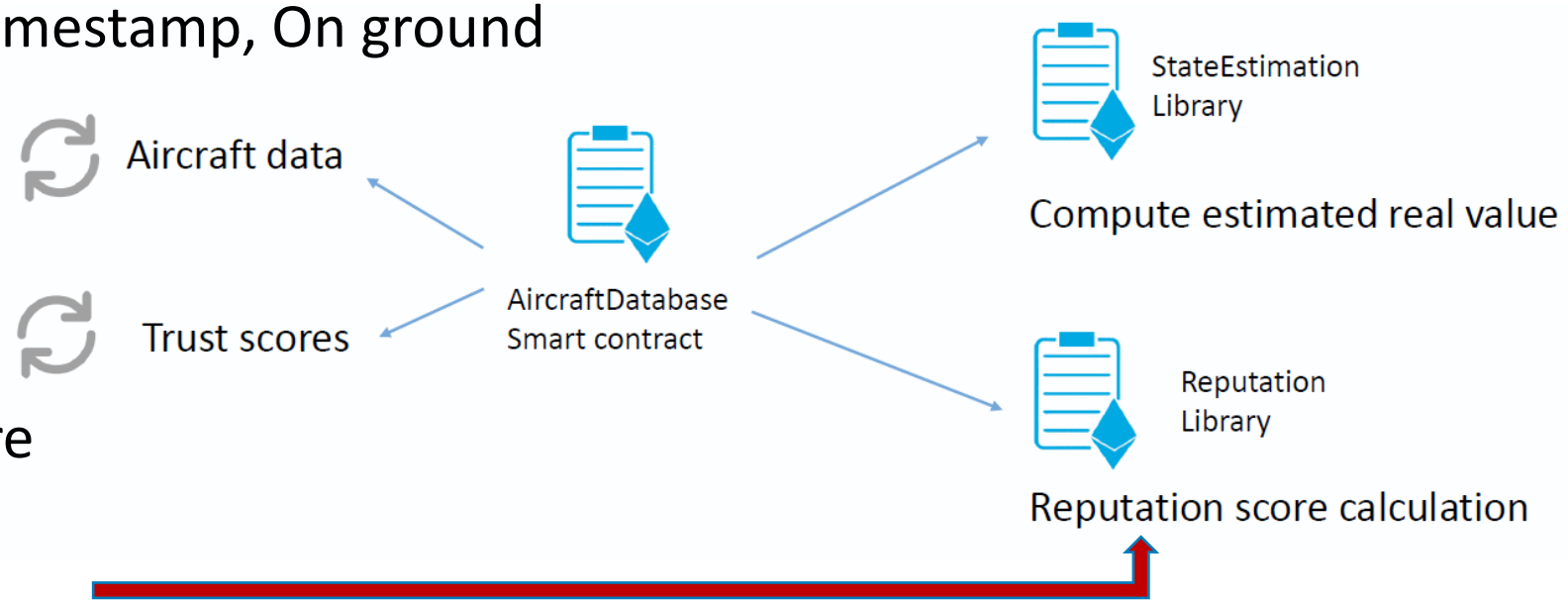




A2 : Distributed Ledger for Sky Tracking Data

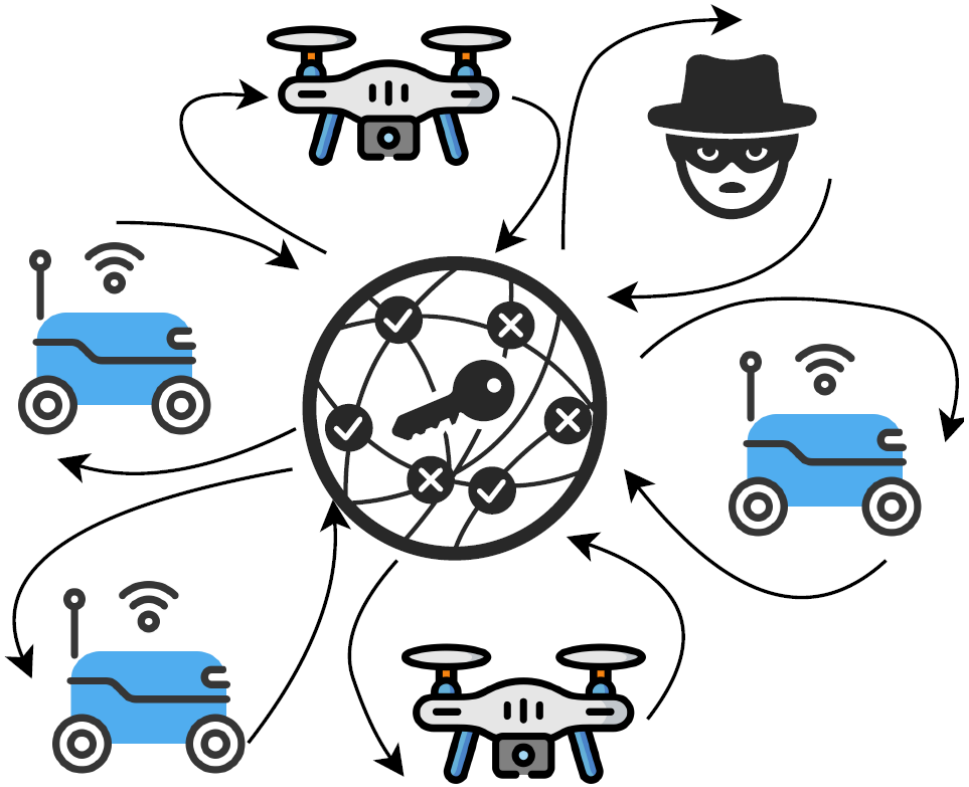
OpenSky network → non-profit network which has been continuously collecting air traffic surveillance data since 2013.
Contributing sensors collect ICAO24 code, Long., Lat., Velocity, True track, Vertical rate, Timestamp, On ground state information, …

Proposed blockchain application :



Main contribution : reputation score

A3 :Decentralized management of drones swarm : Multi-UAVs Context



[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]
[Santos de Campos, M. G. and Ponzoni Carvalho Chanel, C. and Chauffaut, C. and Lacan, J..Towards a Blockchain-Based Multi-UAV Surveillance System, (2021) Frontiers in Robotics and AI, 8. ISSN 2296-9144]

Smart Contracts

POI 1

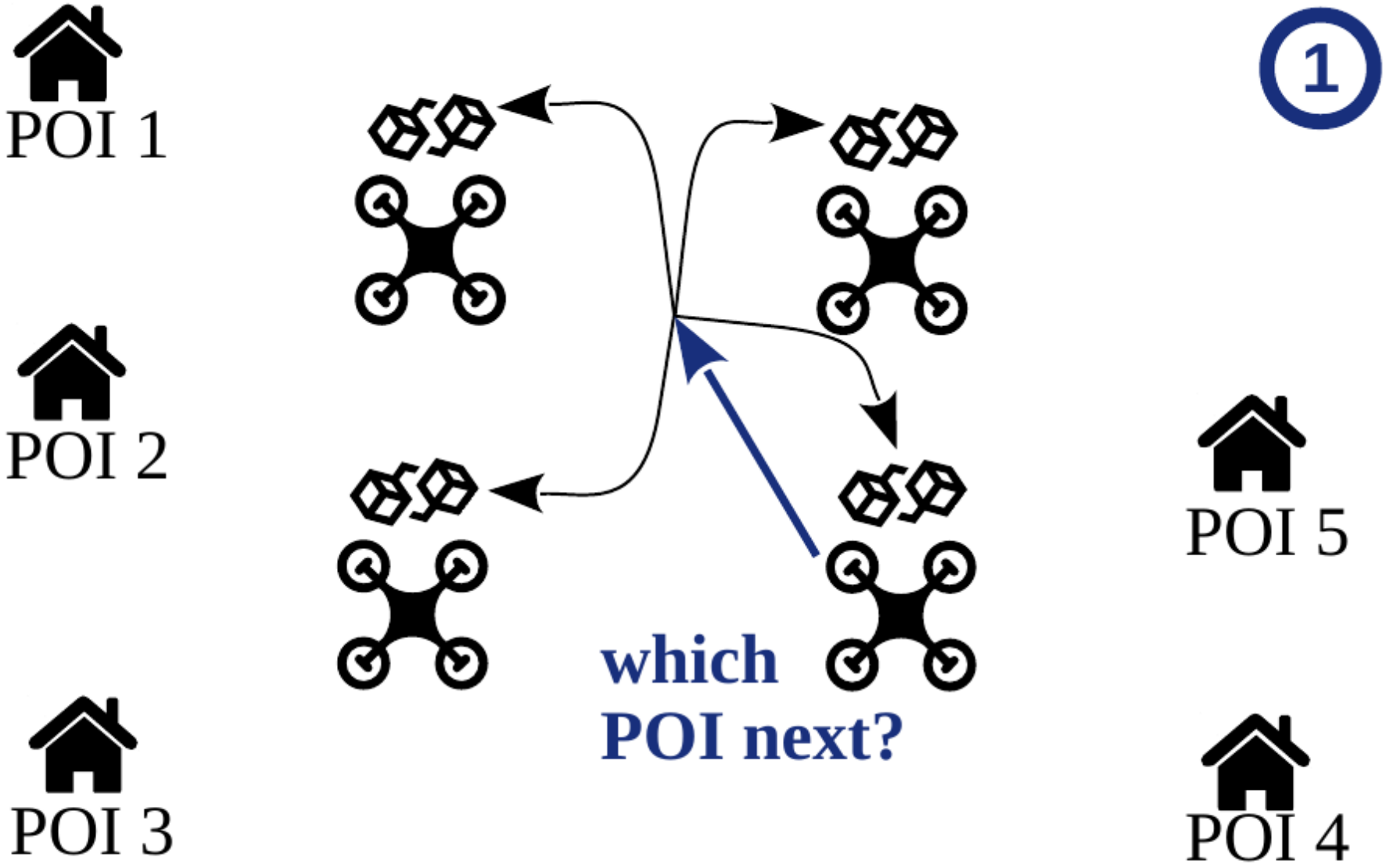
POI 2

POI 5

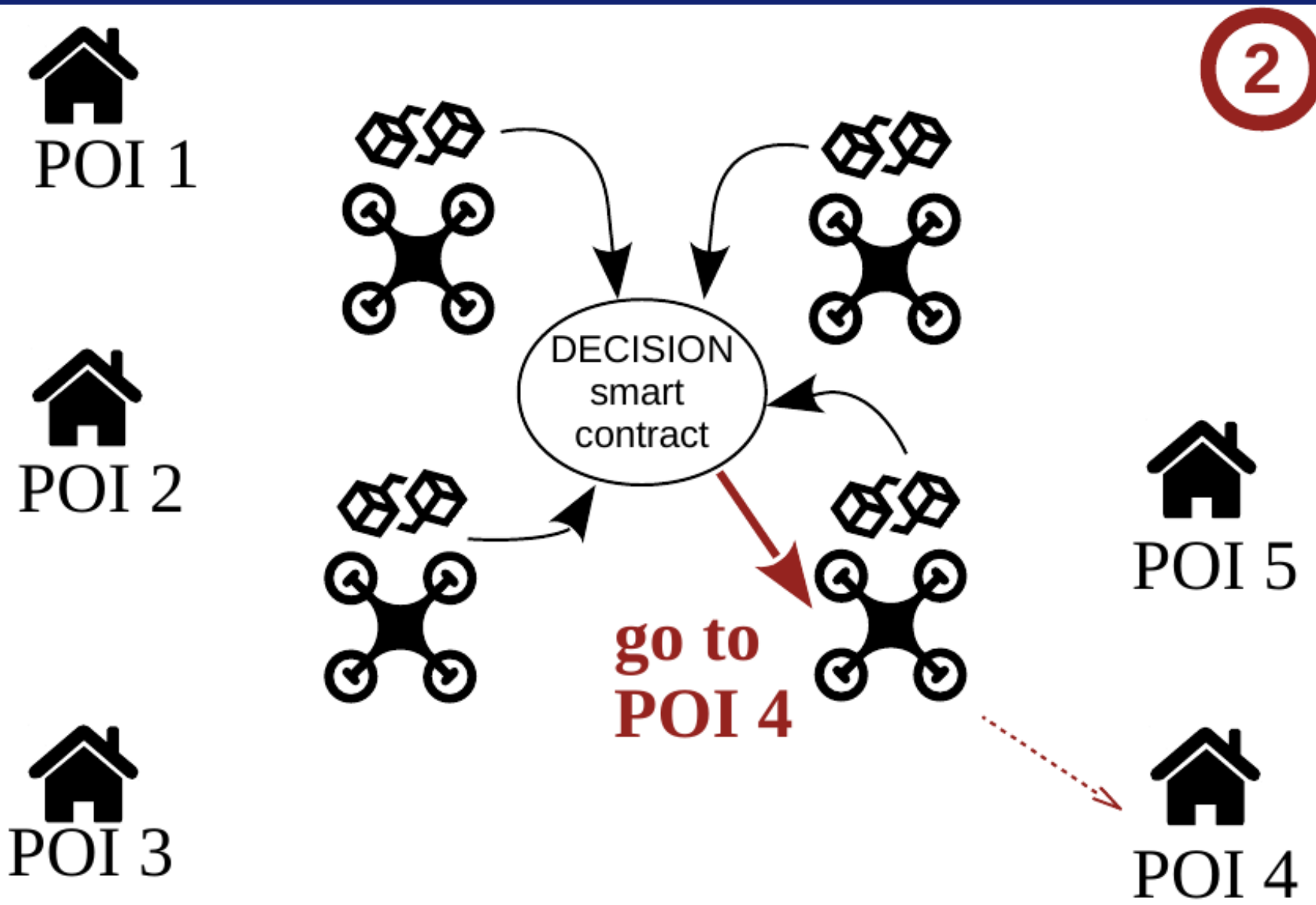
POI 3

POI 4

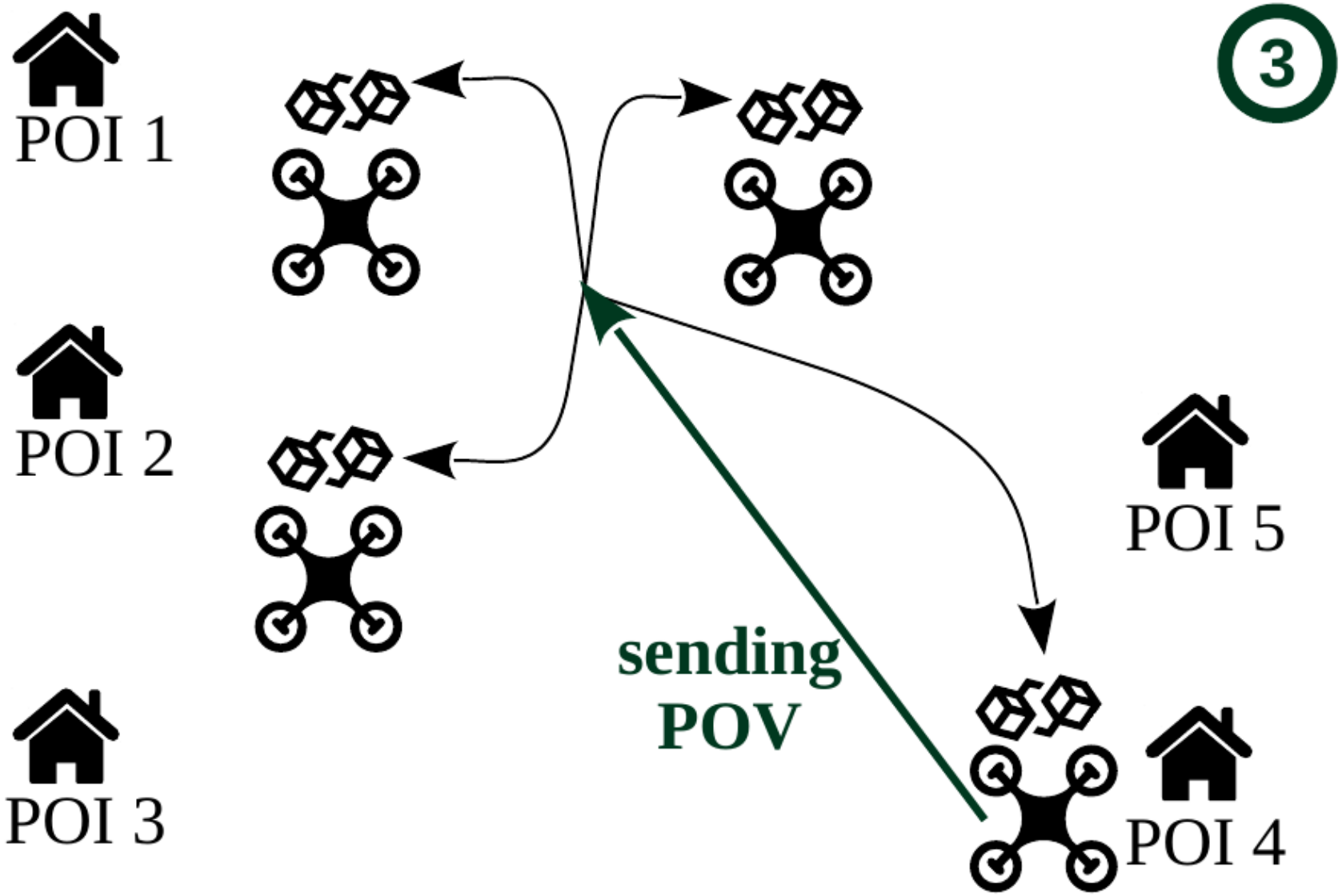
Smart Contracts



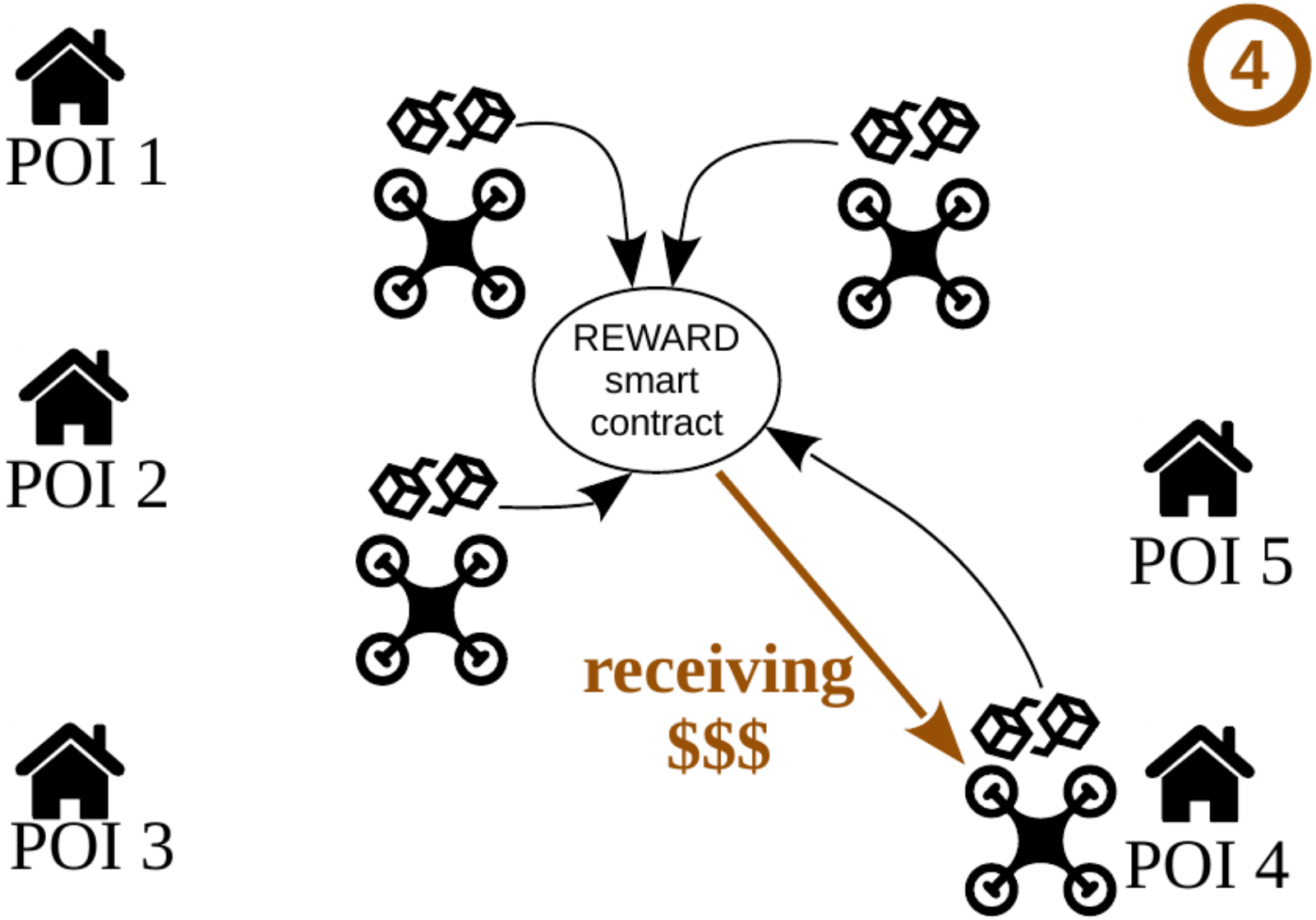
Smart Contracts



Smart Contracts



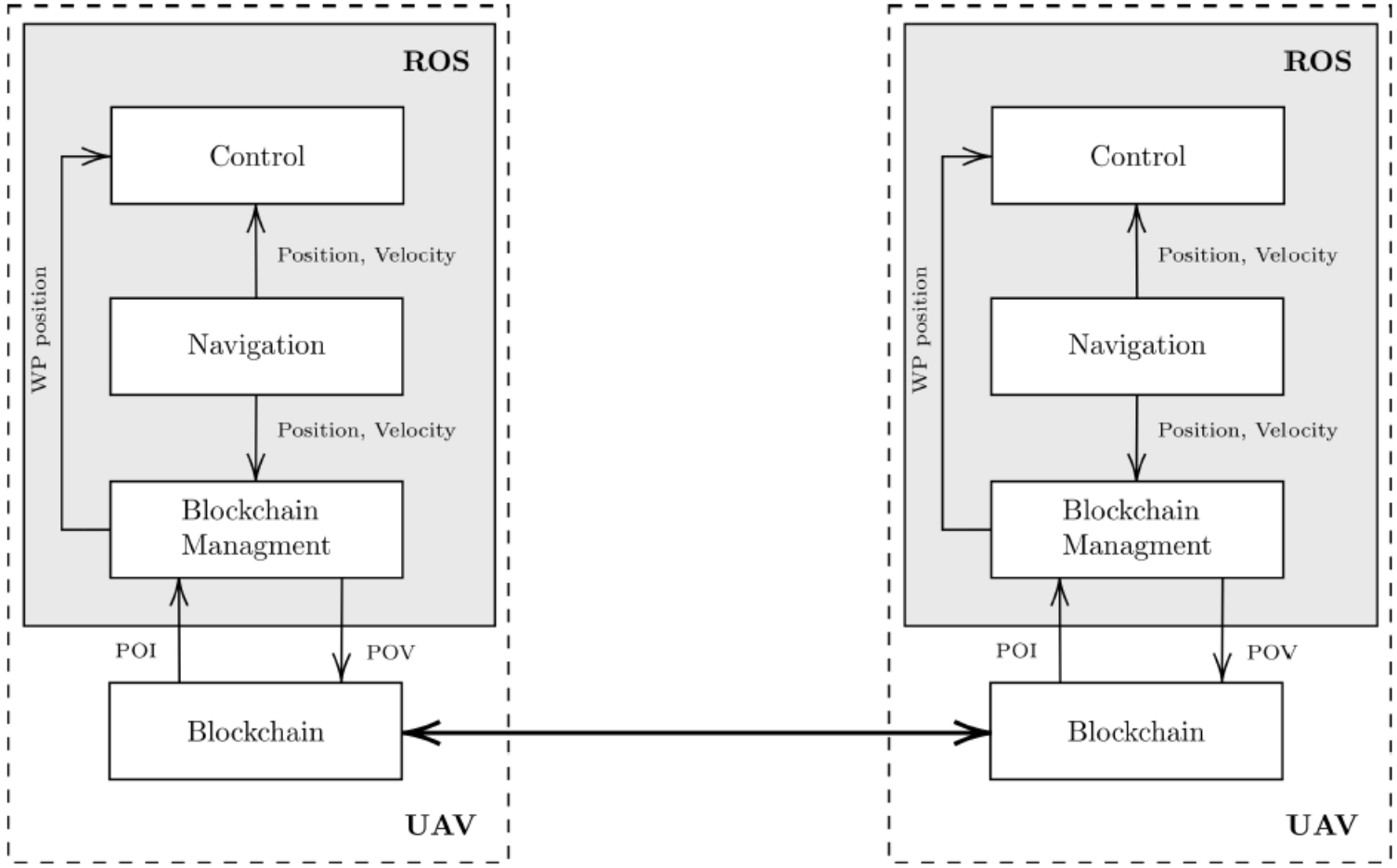
Smart Contracts



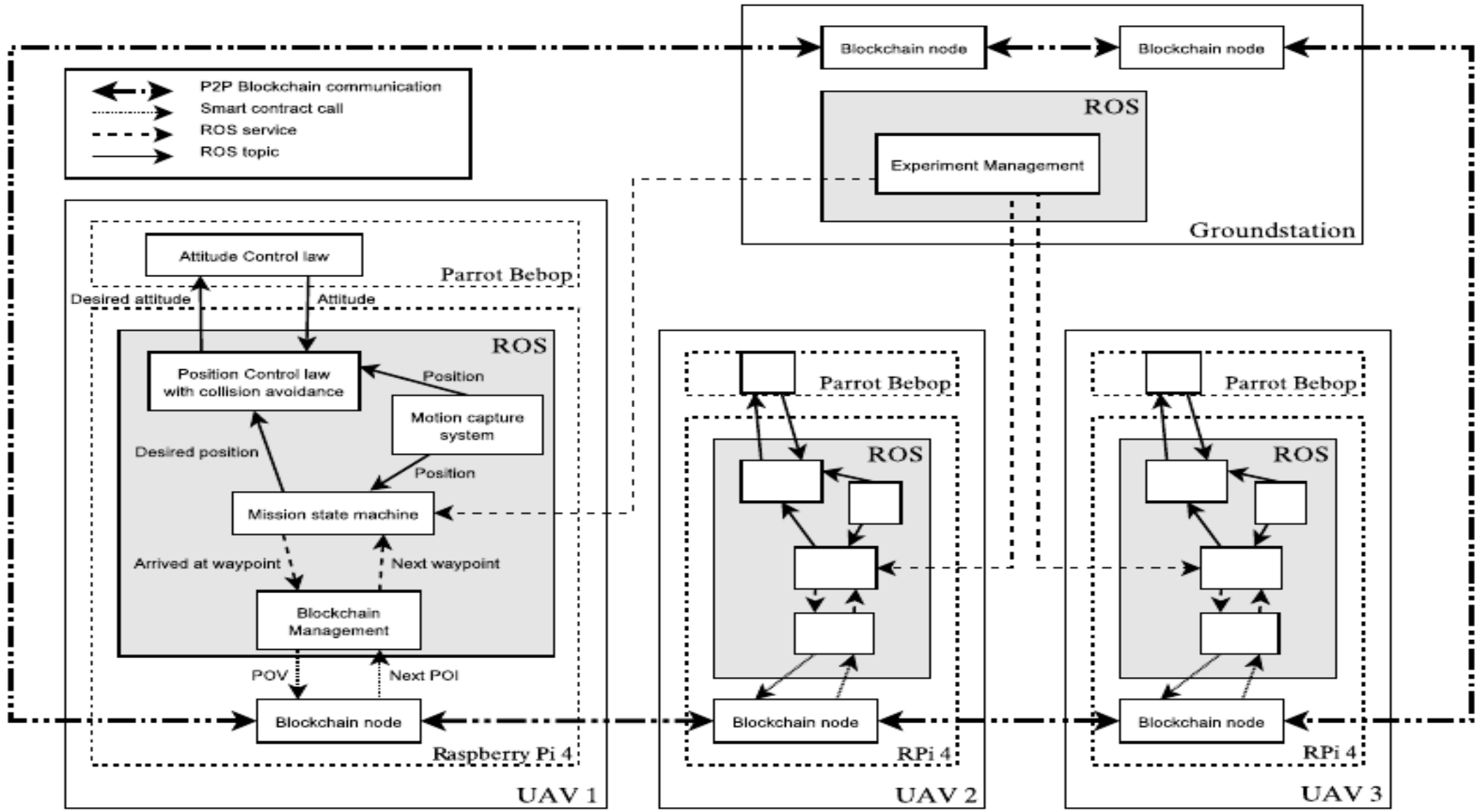
Embedded UAV System

Communication handled by the Blockchain

Each UAV runs a blockchain node



Implementation



Platform

A Mission-Level Resilent Blockchain-based Robotic System

ISAE-SUPAERO

A4 : Last-mile packet delivery

Alphabet

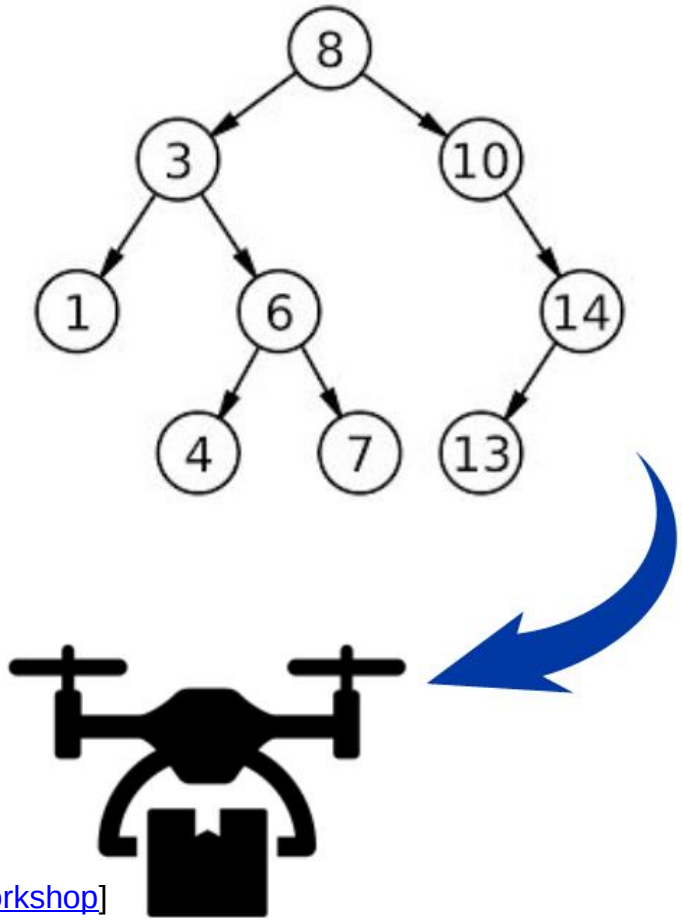
Uber

Shushman Choudhury, Jayesh K. Gupta, Mykel J. Kochenderfer, Dorsa Sadigh, Jeannette Bohg, "Dynamic Multi-Robot Task Allocation under Uncertainty and Temporal Constraints" May 2020,

Decision algorithm

Similarities with the surveillance problem but …
Decision algorithm much more complex

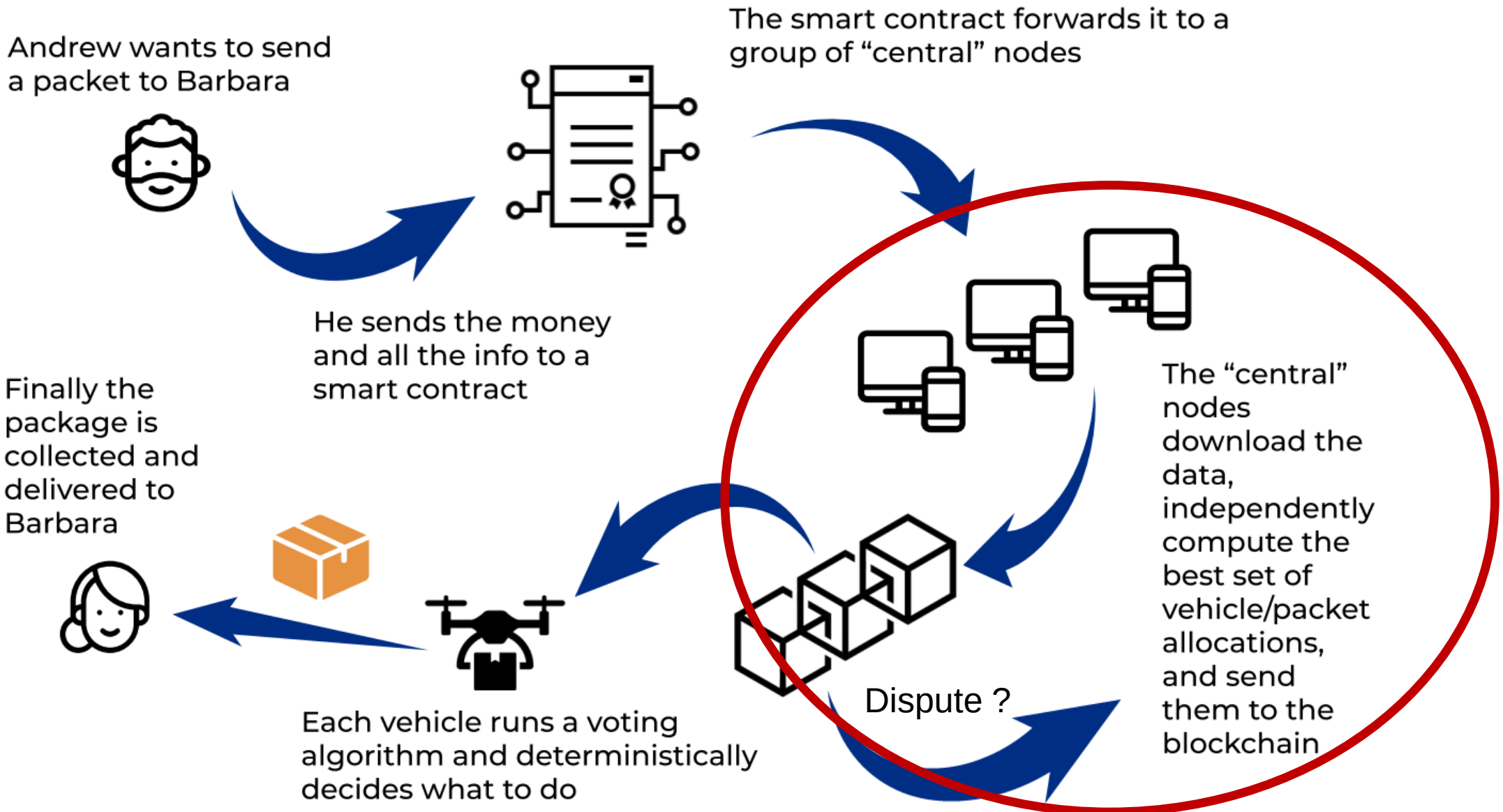
Use of a Monte Carlo Tree Search (MCTS) algorithm for the task allocation



[Sata, B. and Lacan, Jérôme and Ponzoni Carvalho Chanel, C.,
A GA-guided Trial-based Heuristic Tree Search Approach for Multi-Agent Package Delivery Planning, ICAPS-SPARK 2021 Workshop]

[Sata B., Berlanga A., Ponzoni Carvalho Chanel C., Lacan J., Connecting AI-based Oracles to Blockchains via an Auditable Auction Protocol, 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)]

Distributed oracles

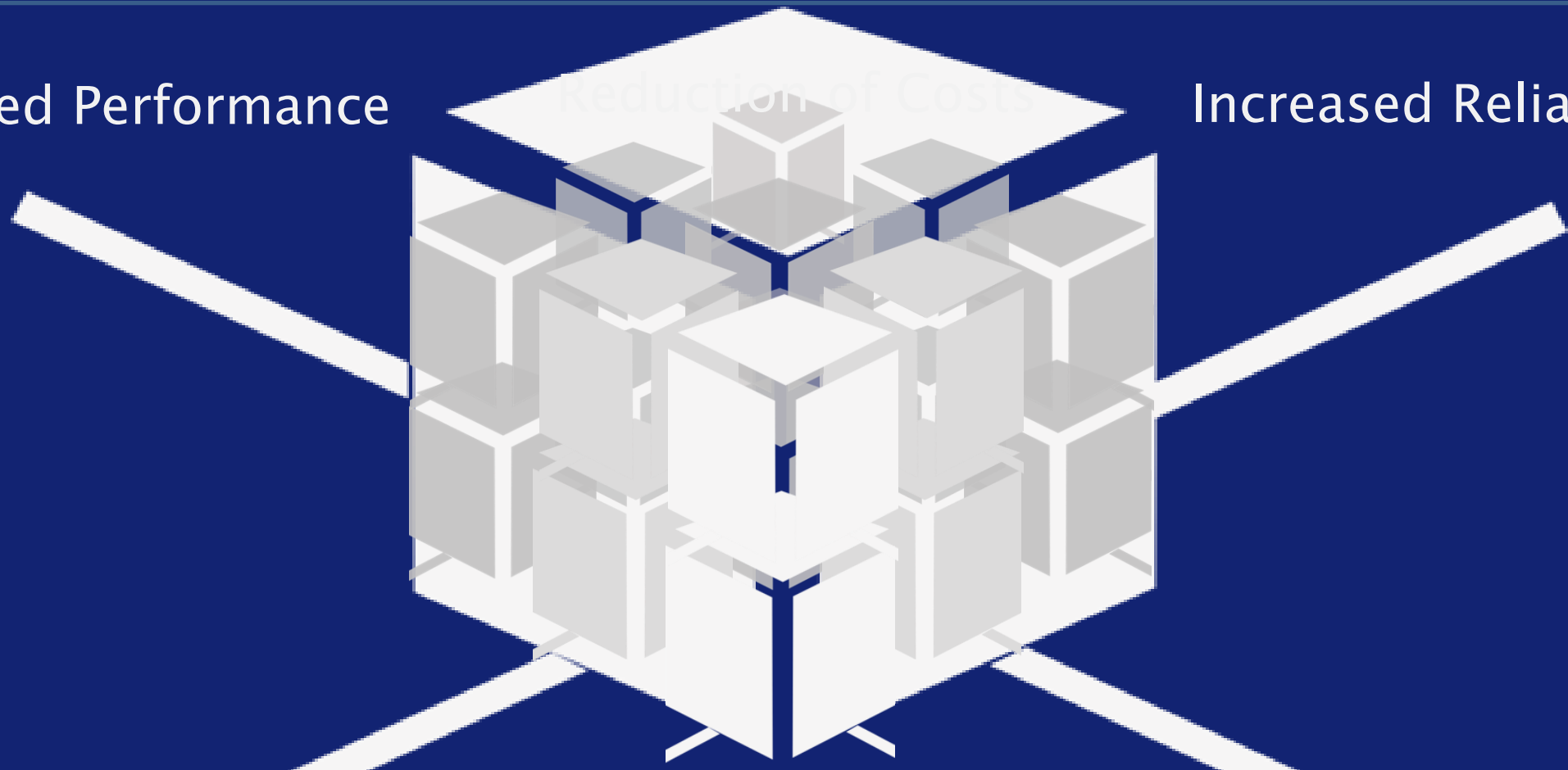


A5 : Blockchain for Fractionated Spacecraft System

Increased Performance

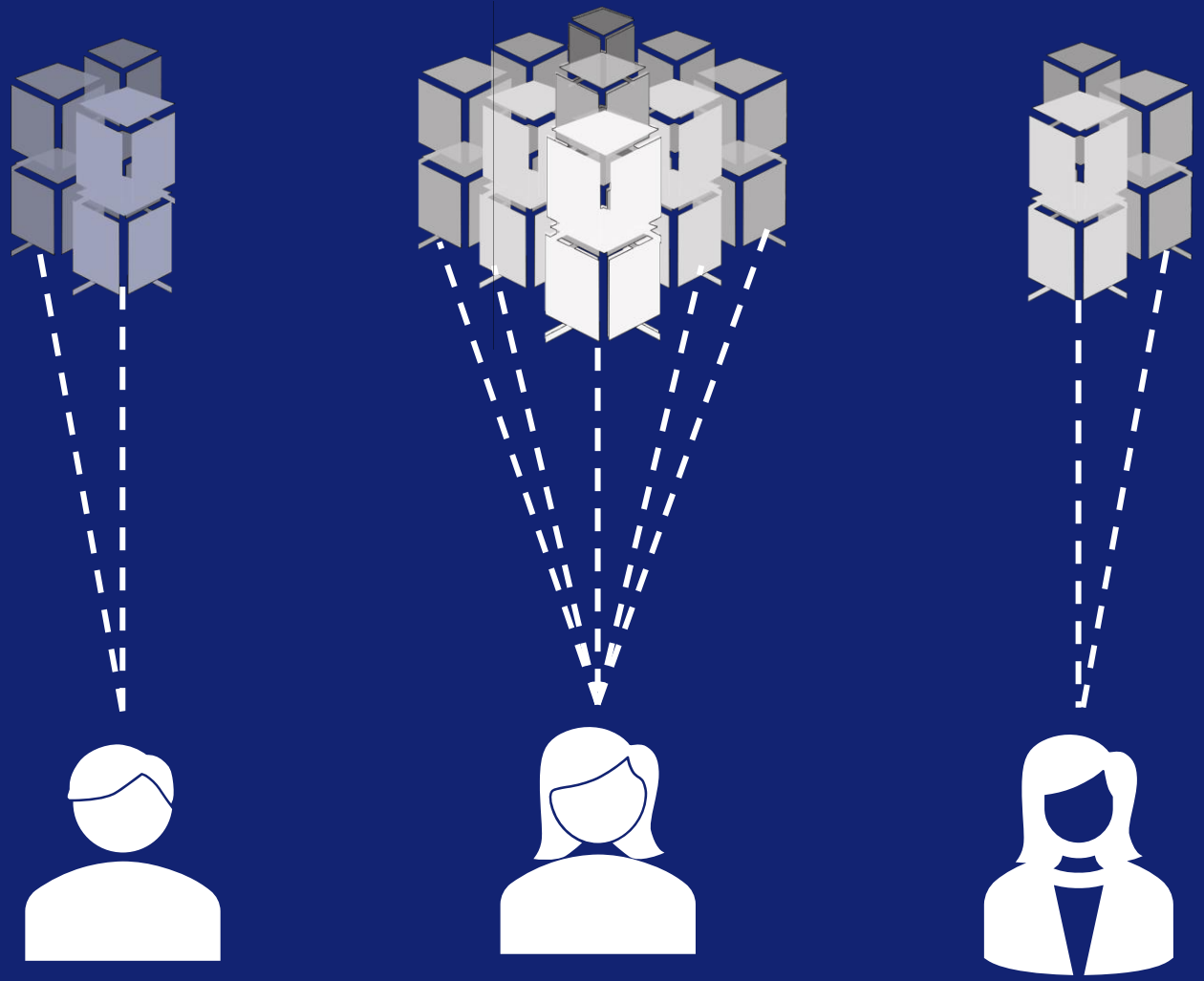
Reduction of Costs

Increased Reliability



Fractionated Spacecraft

Distributed Fractionated Spacecraft



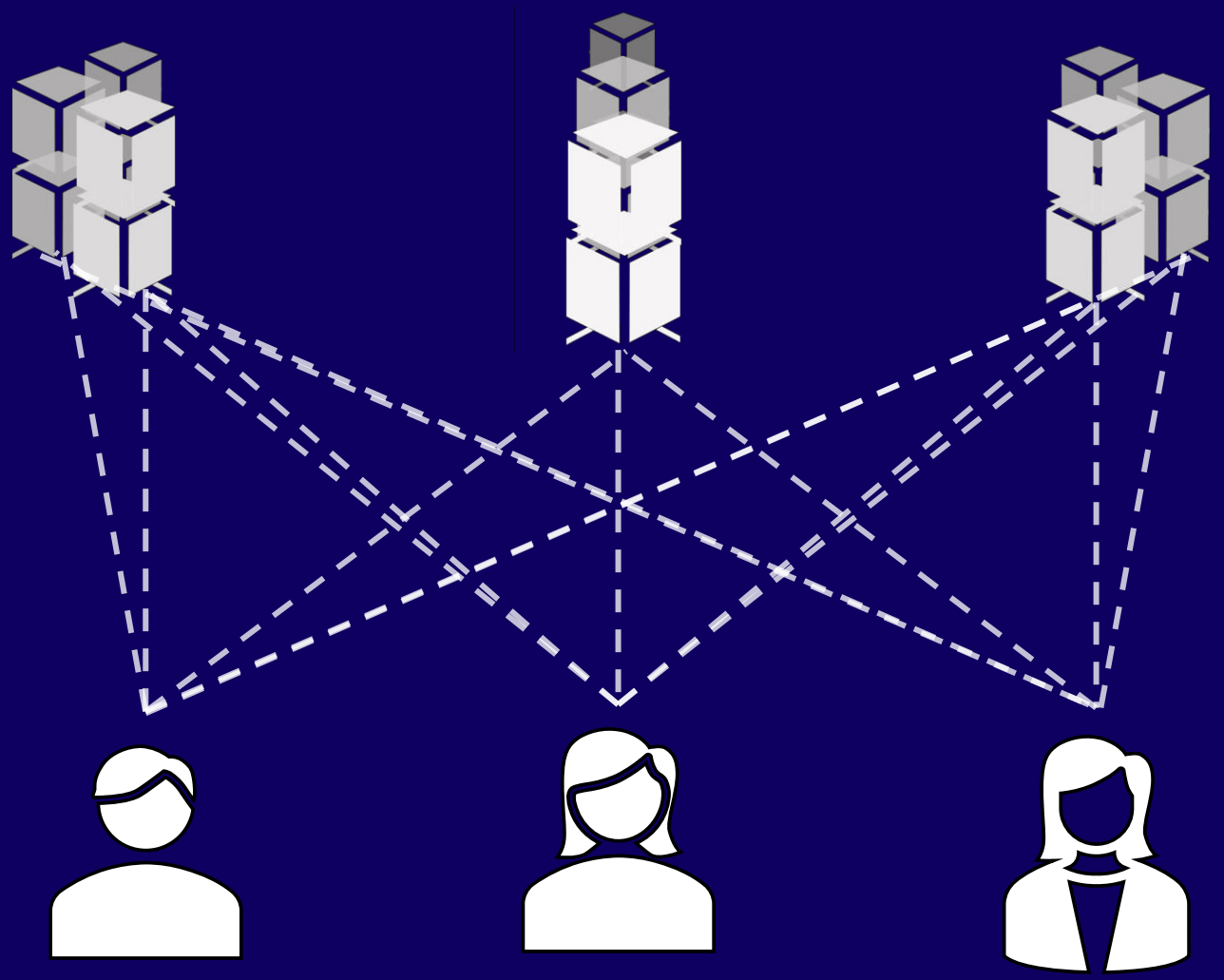
Multiple Entities

Single Entity

Trust Required

Missions

Blockchain-based Fractionated Spacecraft



Multiple Entities

Trustless

Collaborative

Missions

Merci !

Avez-vous des questions ?

Institut Supérieur de l'Aéronautique et de l'Espace
10, avenue Édouard-Belin – BP 54032
31055 Toulouse Cedex 4 – France
T +33 5 61 33 80 80
www.isae-supaero.fr