Projet Fédérateur

Étude et Test de l'Utilisation de la Technologie Blockchain pour la Préservation de la Privacy dans un Contexte Mobile Crowdsensing

Filière : sécurité des systèmes d'information (SSI)

Réalisé par :

AGOULZI Imane

JOUIJATE Rim

Membre de Jury :

Pr. AJHOUN Rachida

Pr. EL BEKKALI Hanane

Encadré par :

Pr. EL BEKKALI Hanane

Mme. MAQOUR Zaina

Année universitaire : 2023-2024

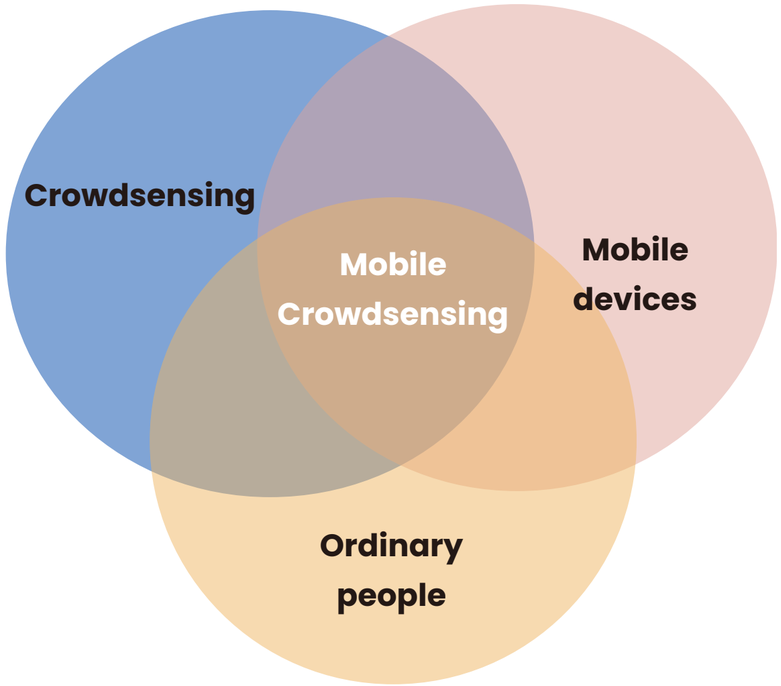
Sommaire

Introduction

Le Mobile Crowdsensing (MCS) implique la collaboration de personnes avec des smartphones, qui partagent collectivement des informations pour mesurer ou cartographier des phénomènes d'intérêt commun.

Le MCS a suscité l'intérêt d'un grand nombre d'acteurs industriels et académiques dans de nombreux **domaines**, parmi lesquels :

- l'étude de la mobilité urbaine
- la surveillance de l'environnement
- la santé
- l'étude des comportements socioculturels
- ...

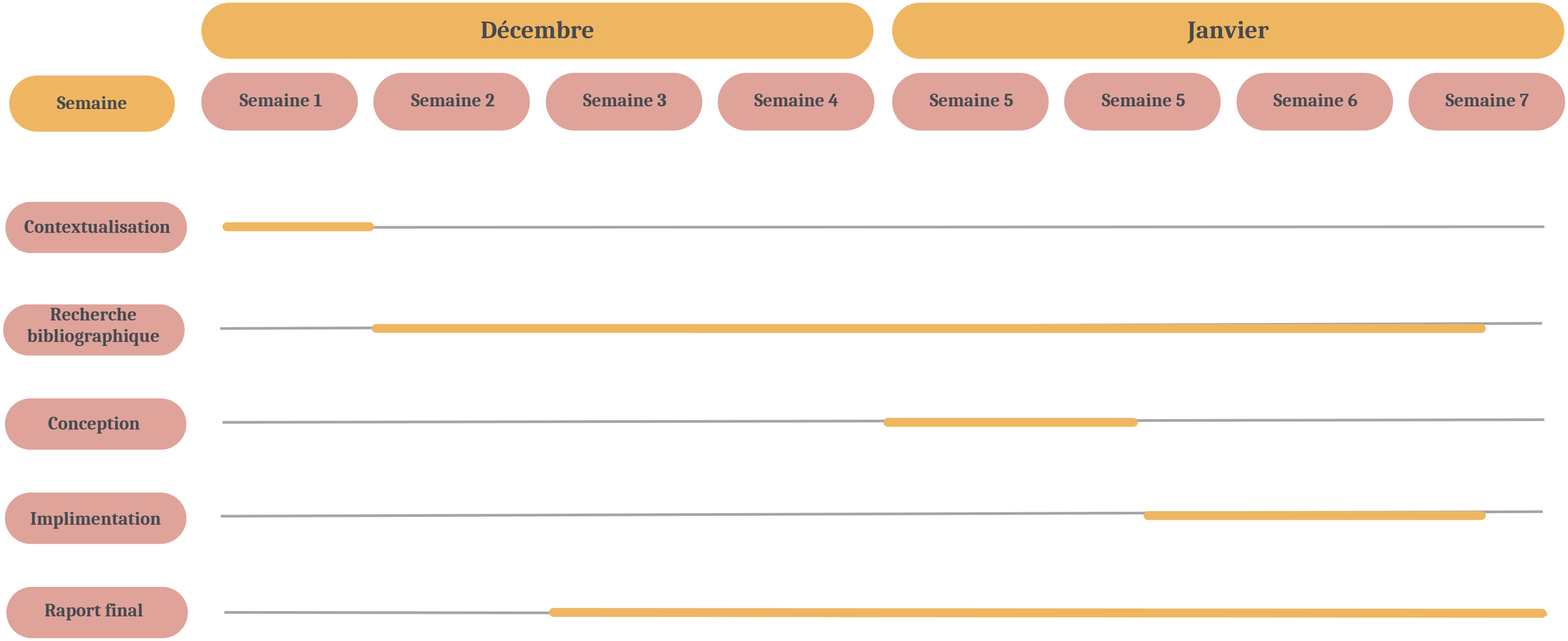


Il offre l'engagement communautaire, la surveillance en temps réel et une collecte de données économique.

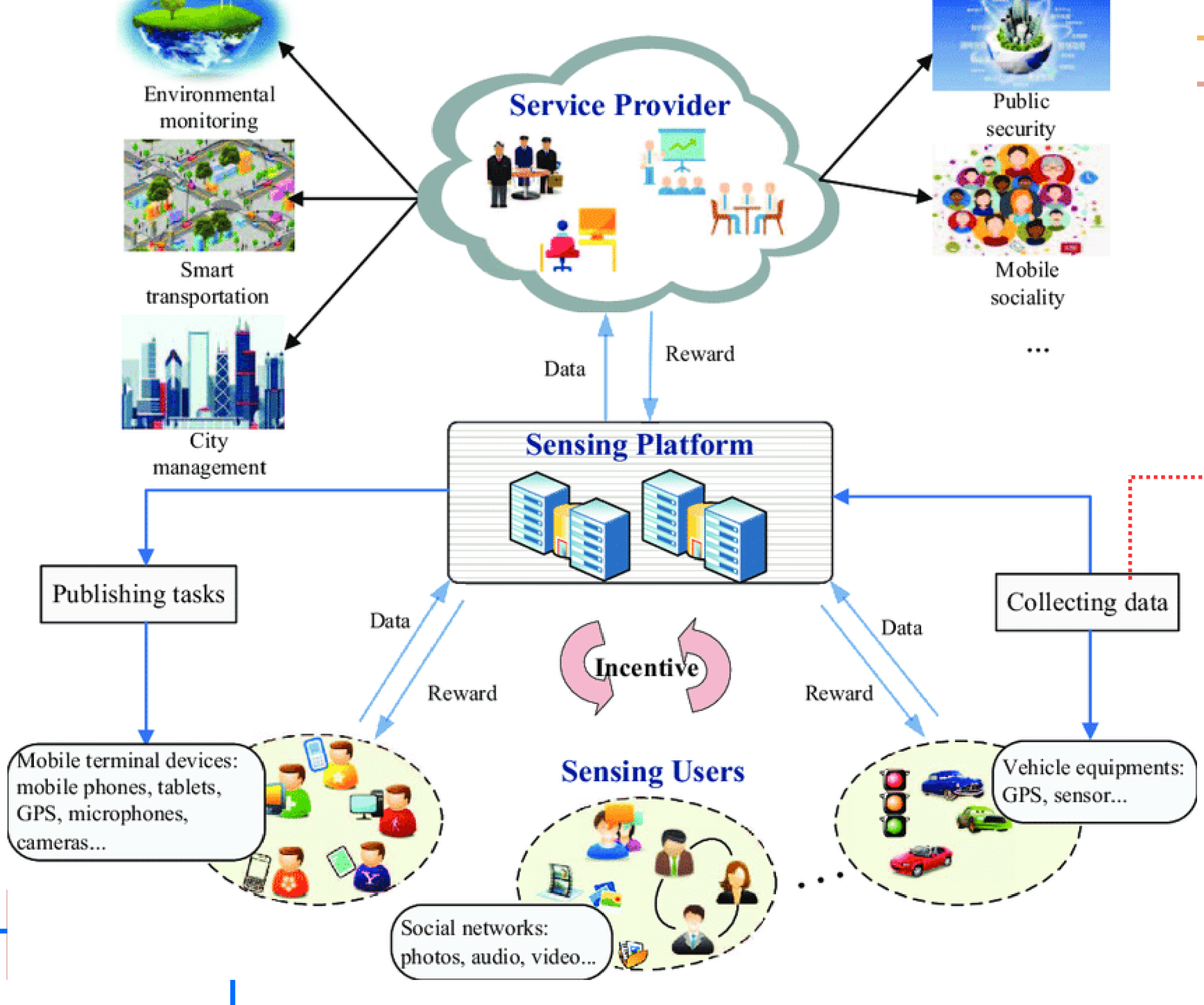
1 Objectifs et planification de projet

- Analyser et comprendre les problèmes spécifiques liés à vie privée dans le contexte du MCS.
- Proposer une solution qui vise à résoudre les défis de MCS en matière de sécurité et vie privée, en intégrant efficacement la technologie Blockchain.
- Mettre en œuvre de manière pratique la solution conçue, à travers une application mobile de MCS basée sur la Blockchain Ethereum.
- Utiliser la réputation des utilisateurs comme condition nécessaire pour leur participation aux activités de MCS.

Planification de projet



2 Contexte de projet



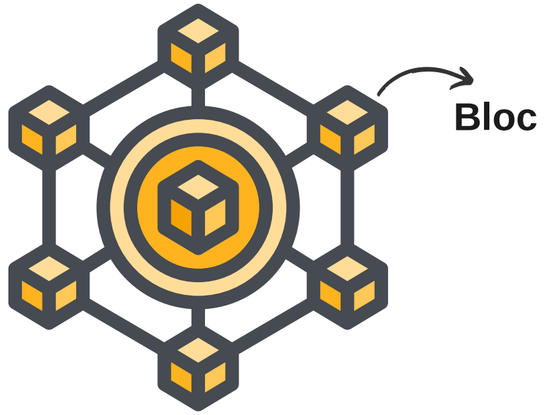
https://www.researchgate.net/figure/System-model-of-mobile-crowdsensing_fig2_328843837

Localisations audios, vidéos, images avec des visages, ...

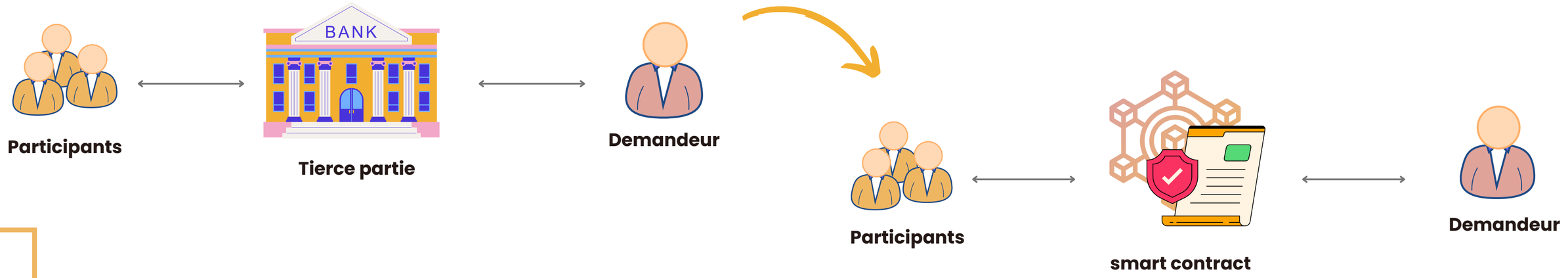
Vie privée

La technologie Blockchain

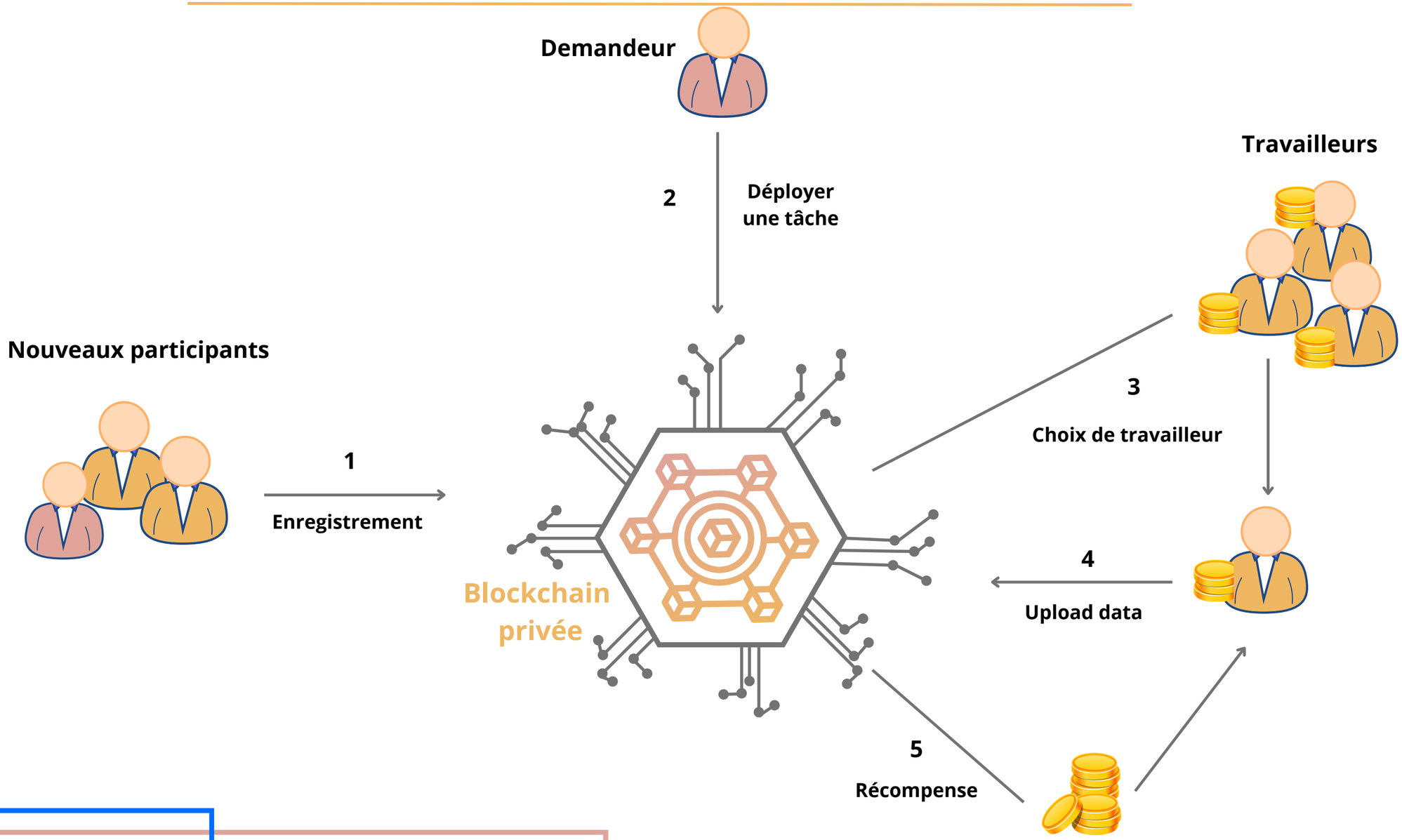
- **Caractéristiques**
  - Distribution
  - Décentralisation
  - Immutabilité
  - Transparence
  - Chronologie et Liens
  - Cryptographie



- **Smart Contract**



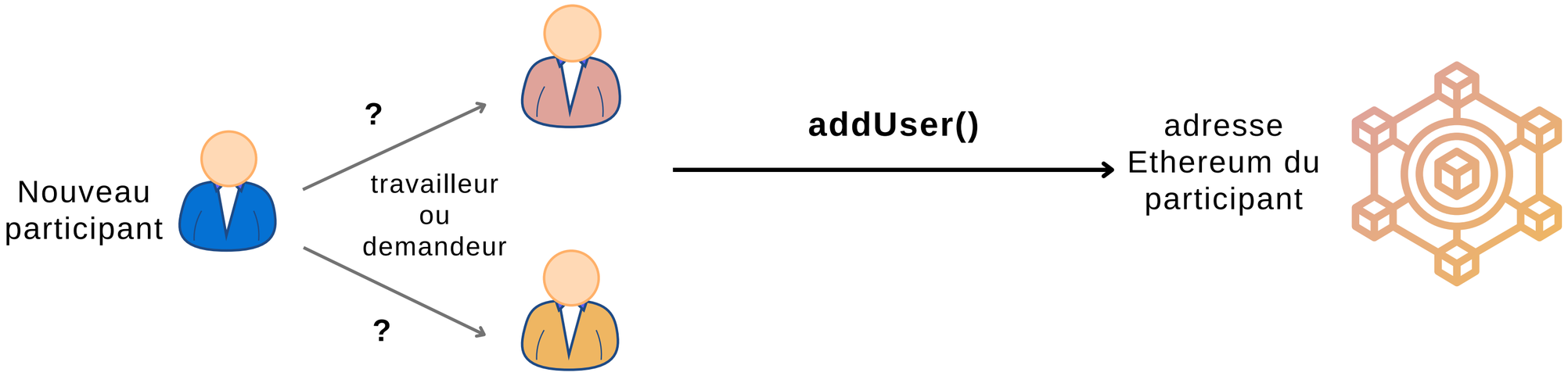
4 Analyse et conception


Demandeur
2
Déployer une tâche
Travailleurs
Nouveaux participants
1
Enregistrement
3
Choix de travailleur
Blockchain privée
4
Upload data
5
Récompense

Contrat d'inscription des utilisateurs

Contrat de création des tâches

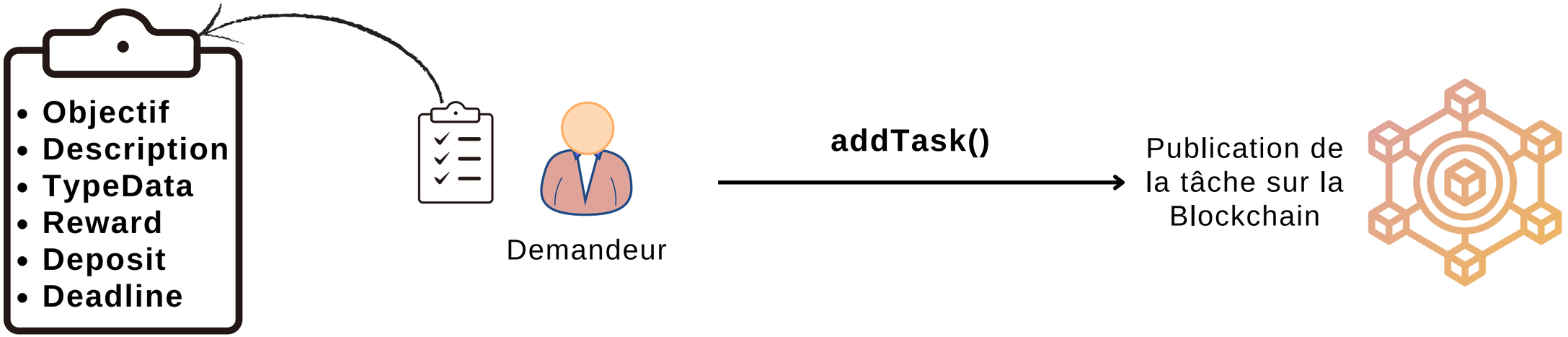
Contrat de gestion de cycle MCS



Contrat d'inscription des utilisateurs

Contrat de création des tâches

Contrat de gestion de cycle MCS

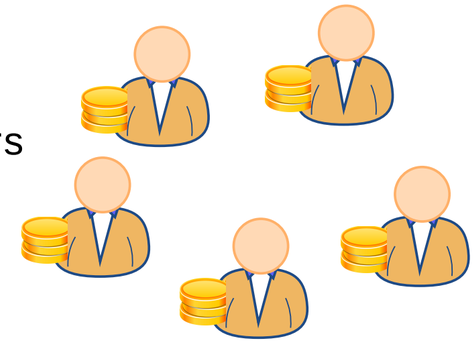


Contrat d'inscription des utilisateurs

Contrat de création des tâches

Contrat de gestion de cycle MCS

Travailleurs

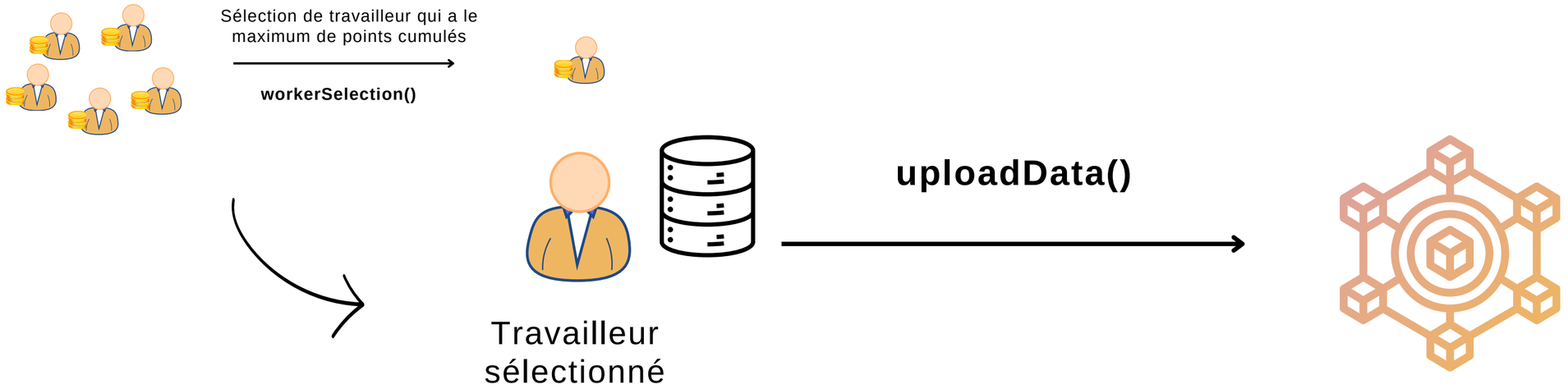


Sélection de travailleur qui a le maximum de points cumulés

workerSelection()

Travailleur sélectionné

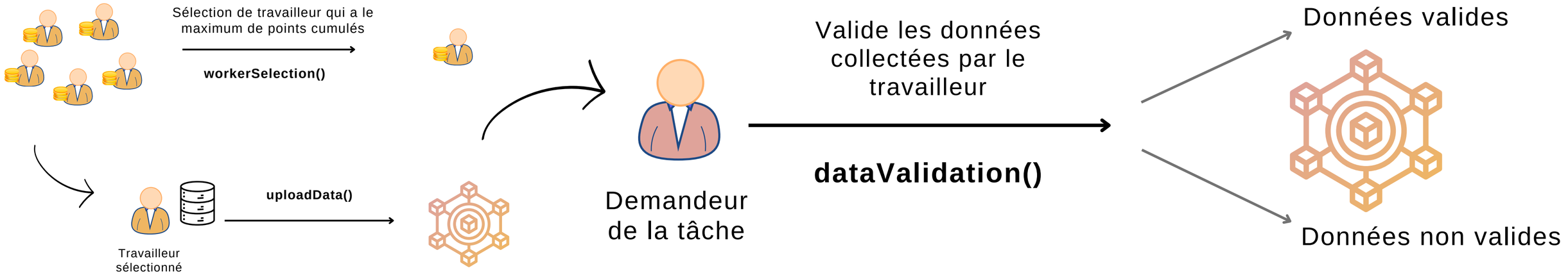
- Contrat d'inscription des utilisateurs
- Contrat de création des tâches
- **Contrat de gestion de cycle MCS**



Contrat d'inscription des utilisateurs

Contrat de création des tâches

Contrat de gestion de cycle MCS



Contrat d'inscription des utilisateurs

Contrat de création des tâches

Contrat de gestion de cycle MCS

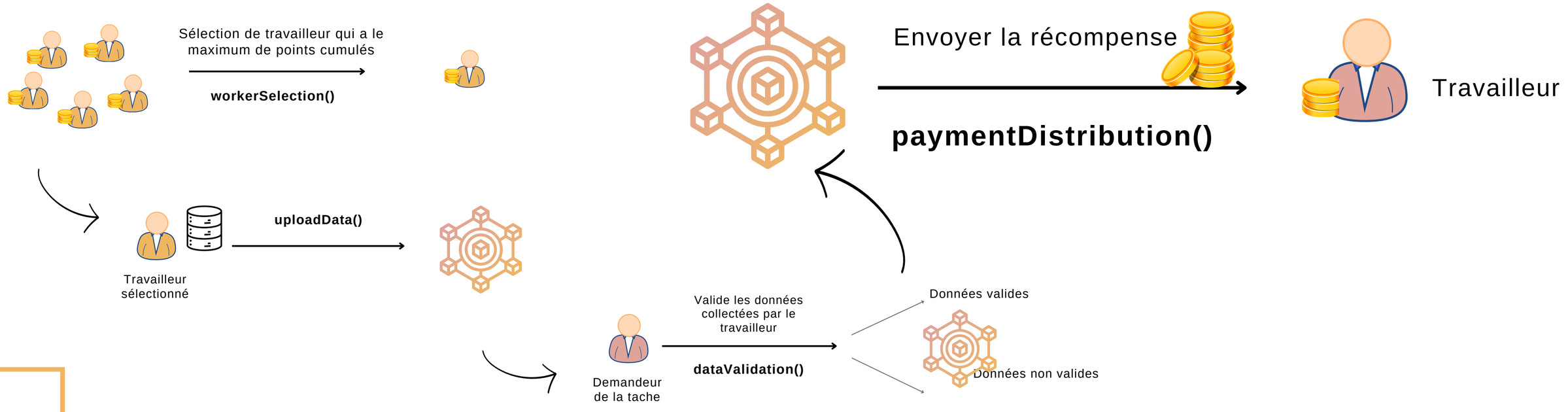
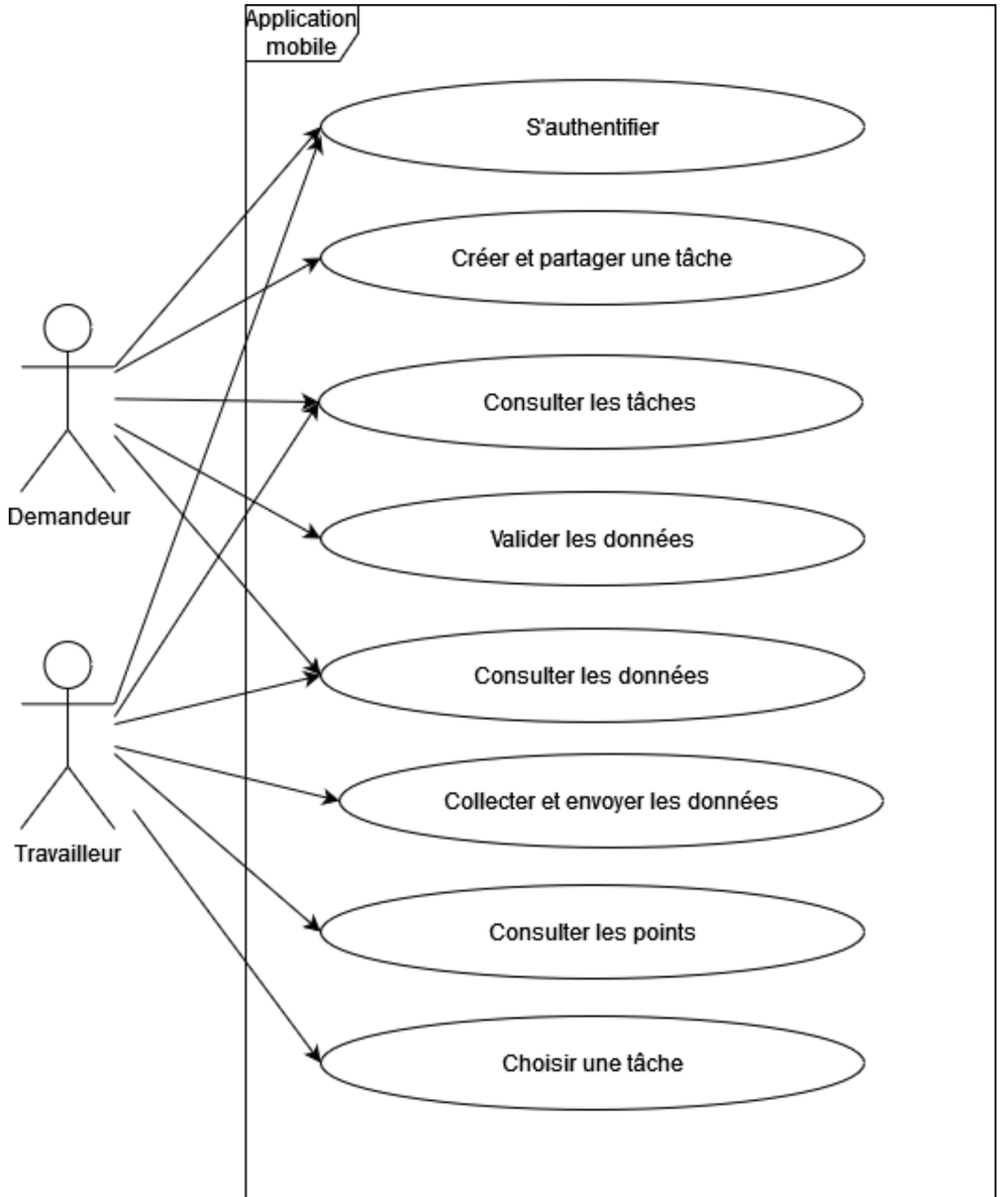
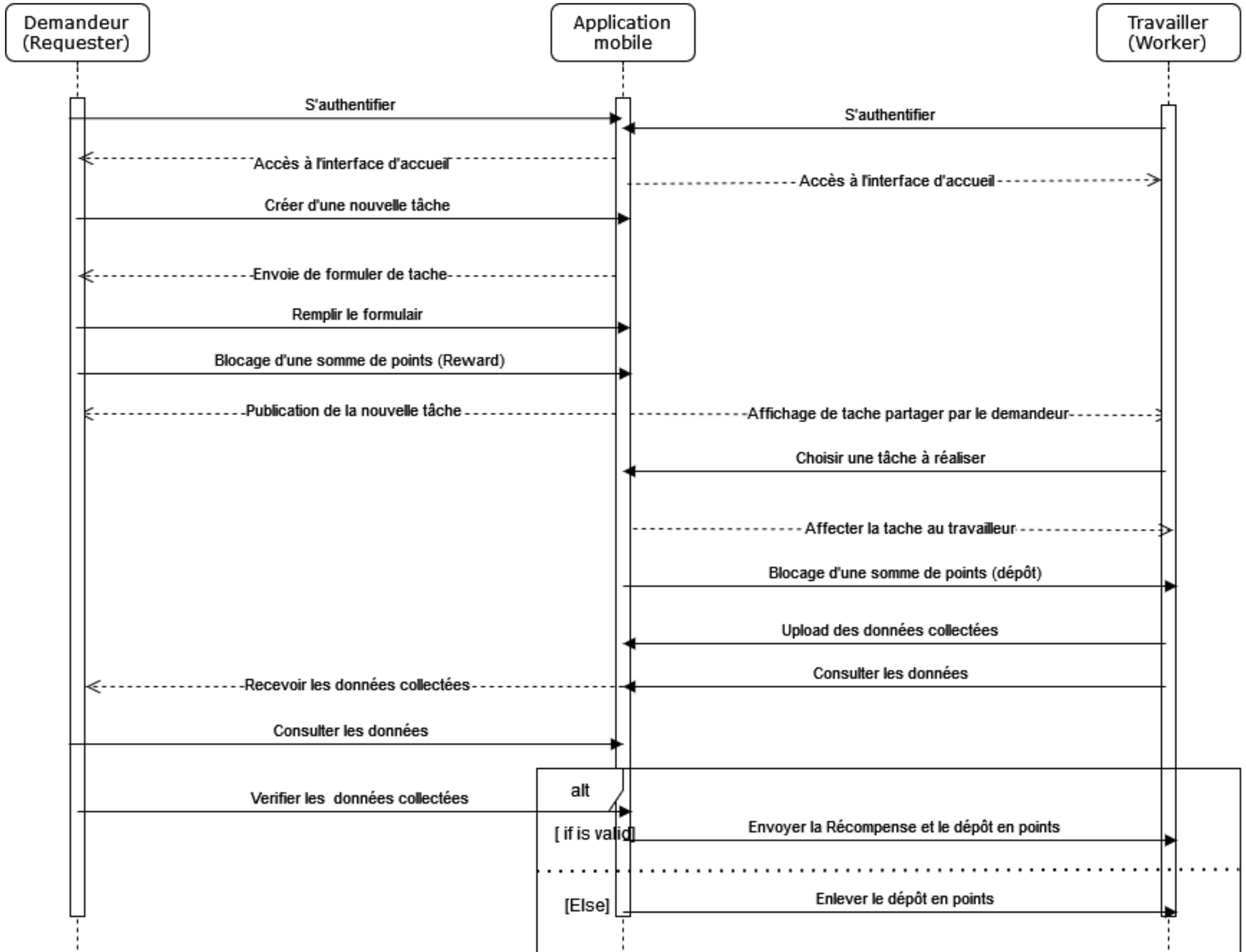


Diagramme de cas d'utilisation

Diagramme de séquence



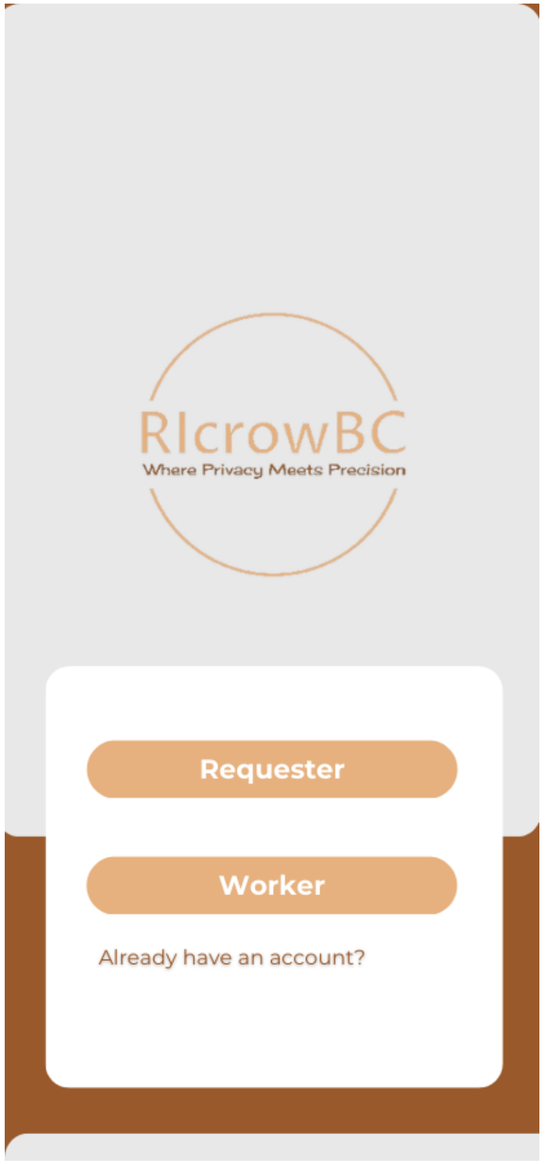
- Diagramme de cas d'utilisation
- **Diagramme de séquence**

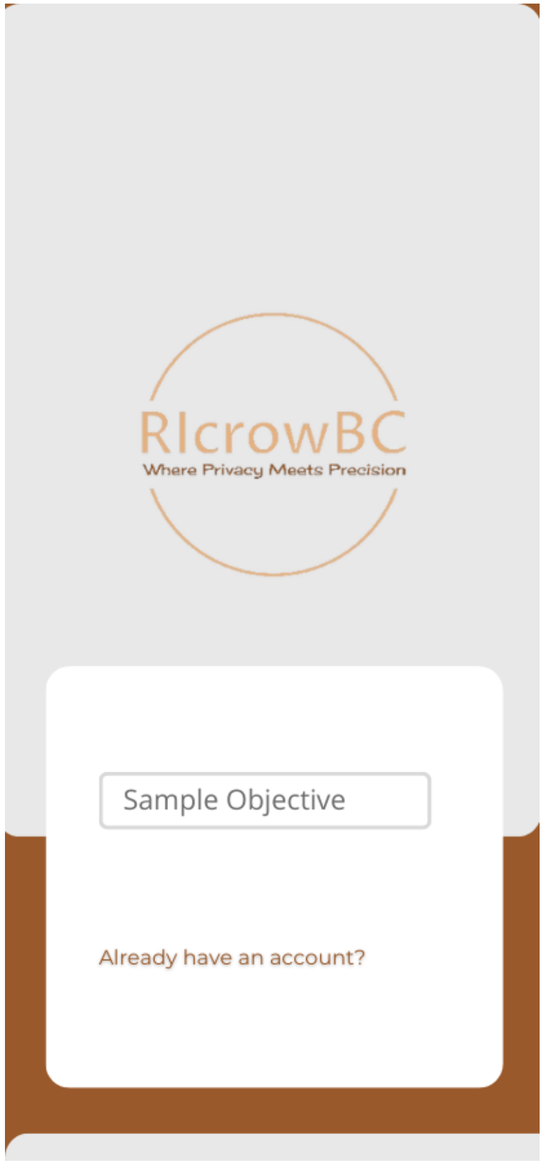


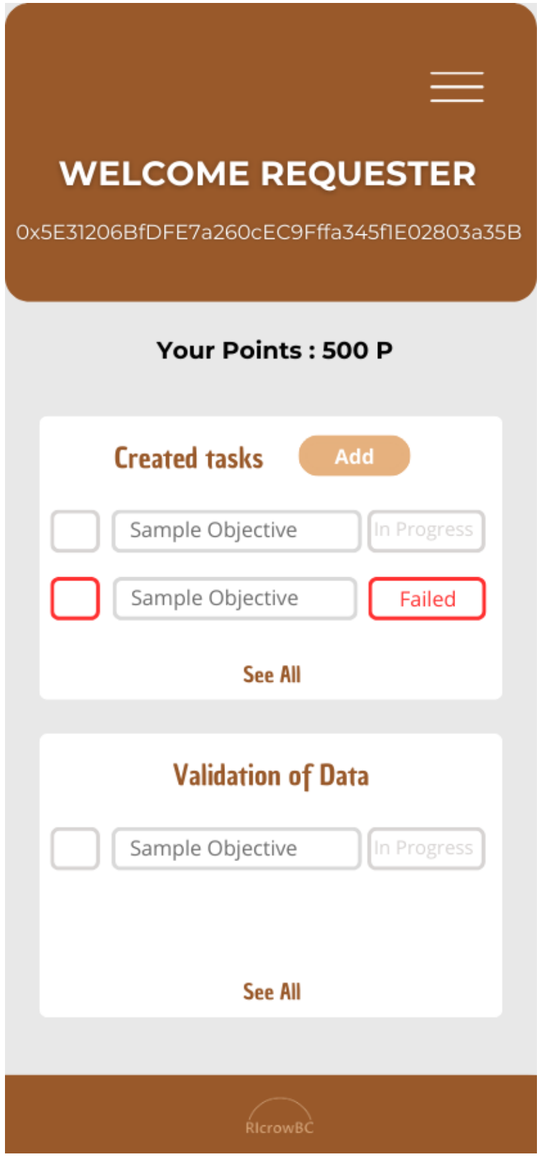
5 Réalisation de projet

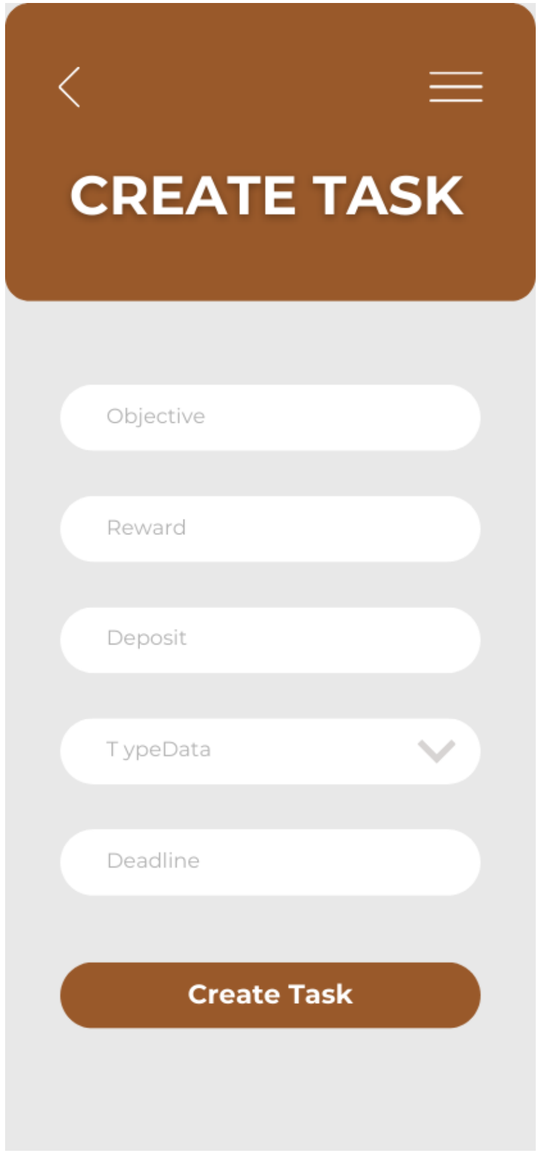
	Ethereum	Permet et le développement d'applications décentralisées et l'exécution de contrats intelligents.
	Solidity （v0.8.17）	Un langage de programmation conçu pour écrire des contrats intelligents sur la plateforme Ethereum.
	Truffle （v5.11.5）	Simplifie la création, le déploiement et les tests de contrats intelligents.
	Ganache （v7.9.1）	Permet de simuler des Blockchains dans un environnement Ethereum local.
	Web3js （v1.10.0）	Une bibliothèque JavaScript qui facilite l'interaction avec la blockchain Ethereum

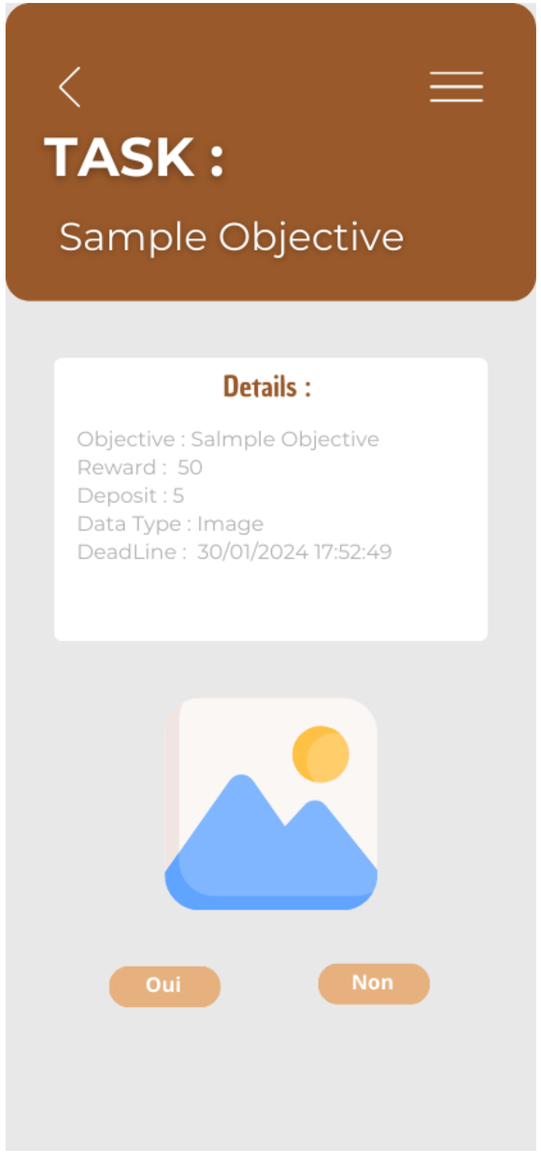
Démo

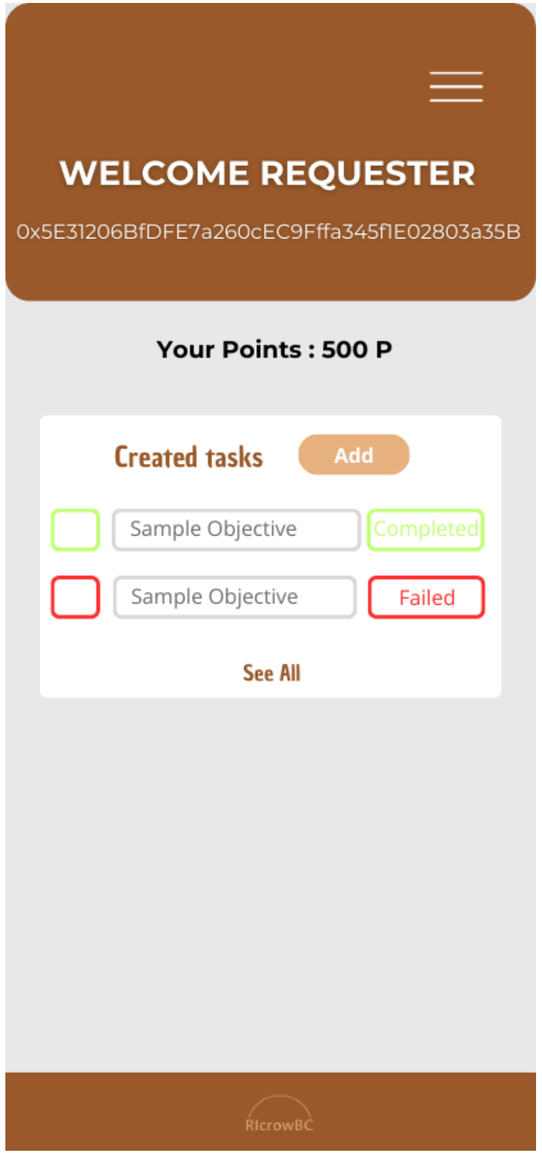

RIcrowBC
Where Privacy Meets Precision
Requester
Worker
Already have an account?

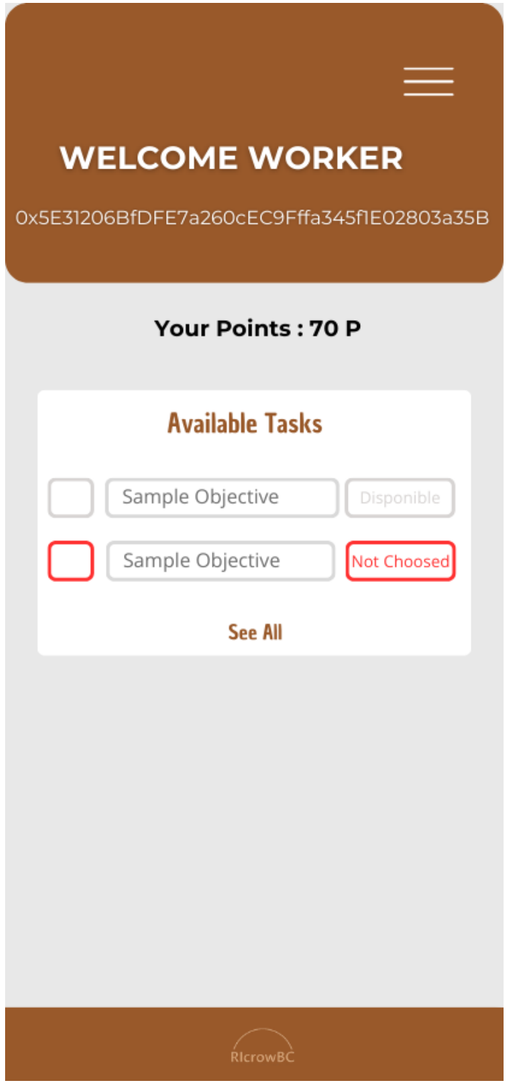

RIcrowBC
Where Privacy Meets Precision
Sample Objective
Already have an account?

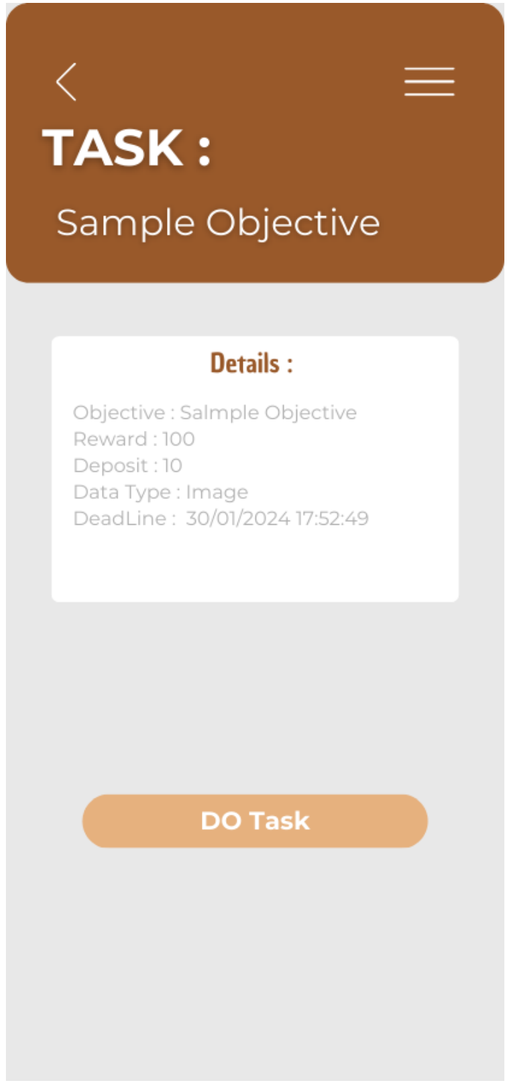

WELCOME REQUESTER
0x5E31206BfDFE7a260cEC9Fffa345f1E02803a35B
Your Points : 500 P
Created tasks
Add
Sample Objective
In Progress
Sample Objective
Failed
See All
Validation of Data
Sample Objective
In Progress
See All
RIcrowBC

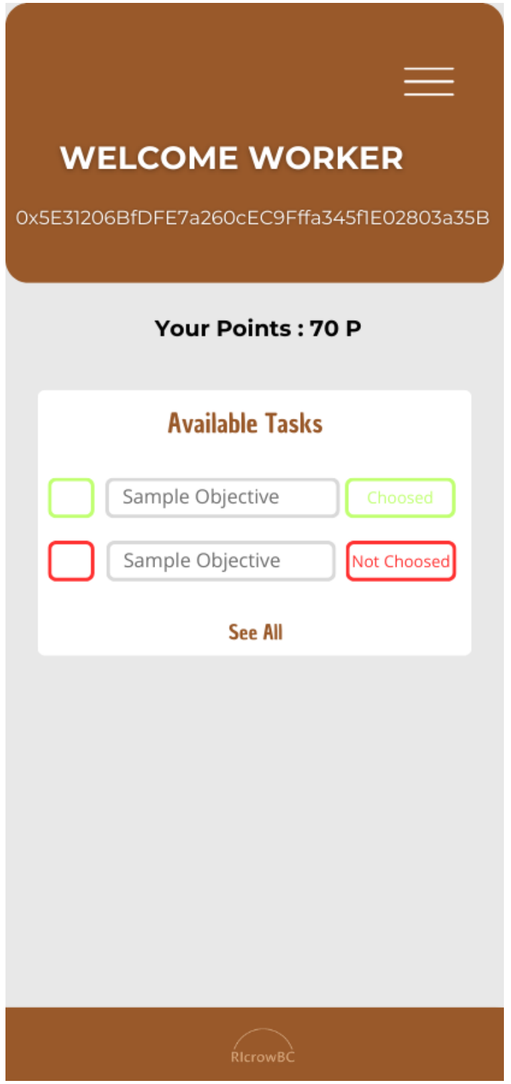

CREATE TASK
Objective
Reward
Deposit
TypeData
Deadline
Create Task

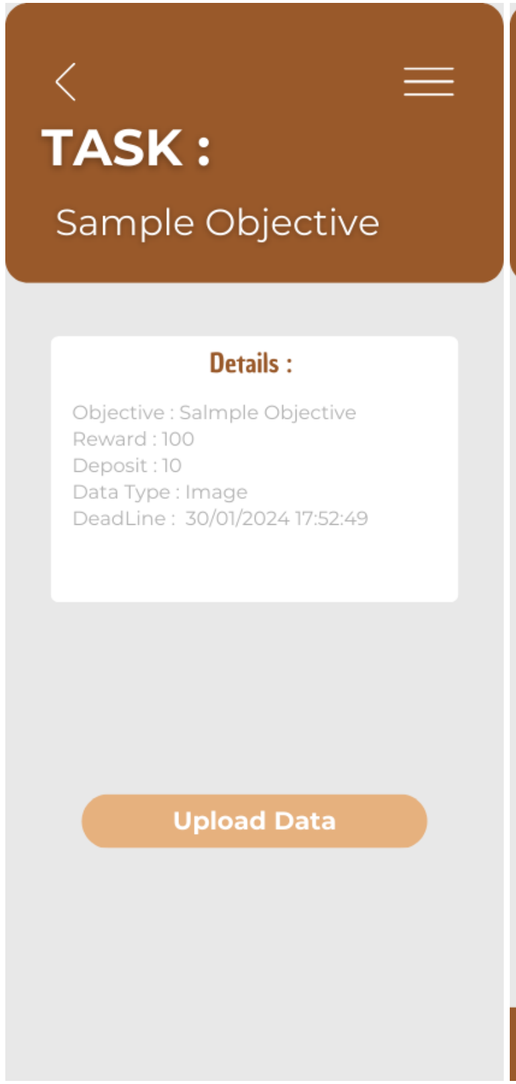

TASK :
Sample Objective
Details :
Objective : Salmple Objective
Reward : 50
Deposit : 5
Data Type : Image
DeadLine : 30/01/2024 17:52:49
Oui
Non

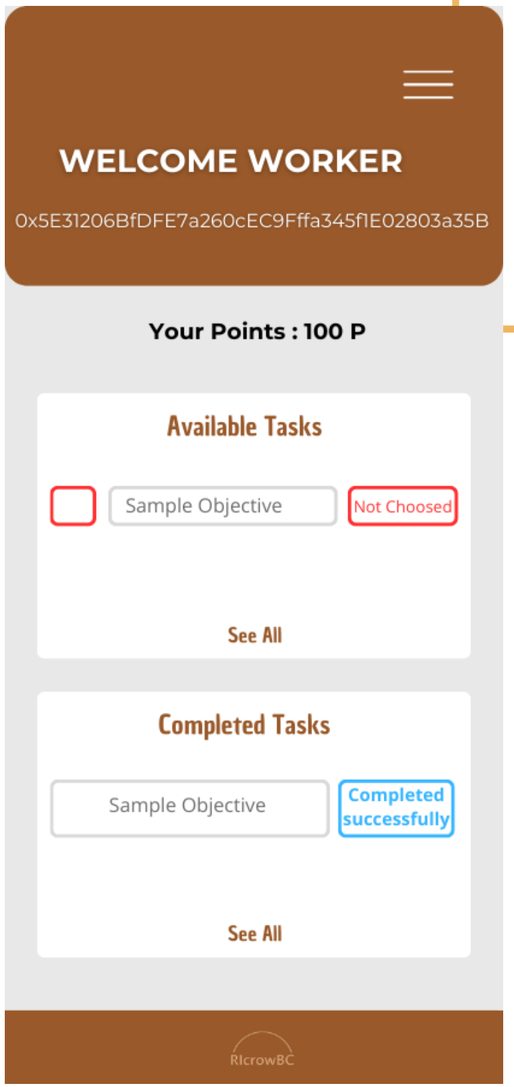

WELCOME REQUESTER
0x5E31206BfDFE7a260cEC9Fffa345f1E02803a35B
Your Points : 500 P
Created tasks
Add
Sample Objective
Completed
Sample Objective
Failed
See All
RIcrowBC


WELCOME WORKER
0x5E31206BfDFE7a260cEC9Fffa345f1E02803a35B
Your Points : 70 P
Available Tasks
Sample Objective
Disponible
Sample Objective
Not Choosed
See All
RIcrowBC


TASK :
Sample Objective
Details :
Objective : Salmple Objective
Reward : 100
Deposit : 10
Data Type : Image
DeadLine : 30/01/2024 17:52:49
DO Task


WELCOME WORKER
0x5E31206BfDFE7a260cEC9Fffa345f1E02803a35B
Your Points : 70 P
Available Tasks
Sample Objective
Choosed
Sample Objective
Not Choosed
See All
RIcrowBC


TASK :
Sample Objective
Details :
Objective : Salmple Objective
Reward : 100
Deposit : 10
Data Type : Image
DeadLine : 30/01/2024 17:52:49
Upload Data


WELCOME WORKER
0x5E31206BfDFE7a260cEC9Fffa345f1E02803a35B
Your Points : 100 P
Available Tasks
Sample Objective
Not Choosed
See All
Completed Tasks
Sample Objective
Completed successfully
See All
RIcrowBC

Conclusion

- Pour améliorer le niveau de la protection de la vie privée des participants aux activités de MCS, une architecture basée sur la Blockchain Ethereum a été implémentée exploitant le potentiel des contrats intelligents.

- L'application mobile conçue met en pratique cette architecture, en illustrant les différentes phases de cycle de MCS.

Perspectives

- Il est possible d'établir la communication entre l'application mobile conçue et les contrats intelligents créés et déployés au niveau de notre Blockchain à travers la libraire web3j.

- Des algorithmes de l'intelligence artificielle pourront être intégré pour rendre le processus de validation de données collectées plus précis et plus efficace.

- Le stockage sur la Blockchain est limitée par rapport aux quantités de données collectées à travers le MCS, donc il est préférable d'externaliser le stockage de ses données en protégeant leur confidentialité et leur intégrité grâce aux mécanismes cryptographiques.

MERCI POUR VOTRE ATTENTION