



**BikeChain**

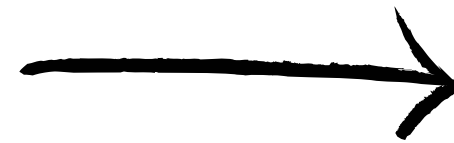
# **COMPRENDRE LA BLOCKCHAIN : POC**

- Edward Lucyszyn
- Elisabeth El Murr
- Eloïse Baril
- Luca Orlandi
- Sakina Boulegroun
- Wolfgang Walter



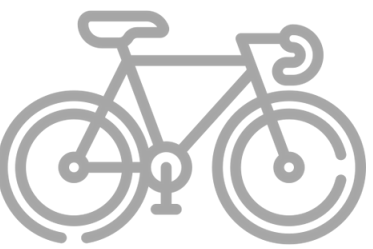
# CONTEXTE

**Conscience écologique  
grandissante  
Transport ~30% des eGES en  
France (2022)**



**Mobilités douces : plus de  
vélos/trottinettes**

**Dans certains pays, un système d'enregistrement des numéros de série des vélos existe déjà,  
cependant il est primitif et peu efficace.**





# PROBLEMES

**~400.000 vélos volés chaque année en France**

**~1/2 déclare le vol à la police ou la gendarmerie**

**Reventes illégales**

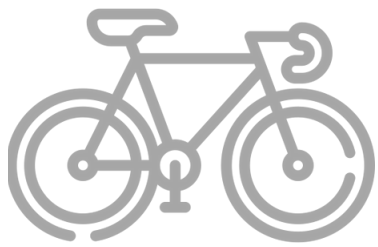


# OBJECTIFS

**Créer un système de vente de vélo qui atteste du parcours de chaque vélo**

**Décourager les reventes de vélos volés**

**Certifier l'origine du vélo**





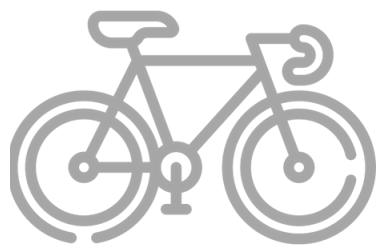
# AVANTAGES DE LA BIKECHAIN



**Vérifier la propriété  
de manière  
transparente  
(immutabilité, accès  
partagé),**

**Créer un historique  
du parcours d'un vélo  
donné**

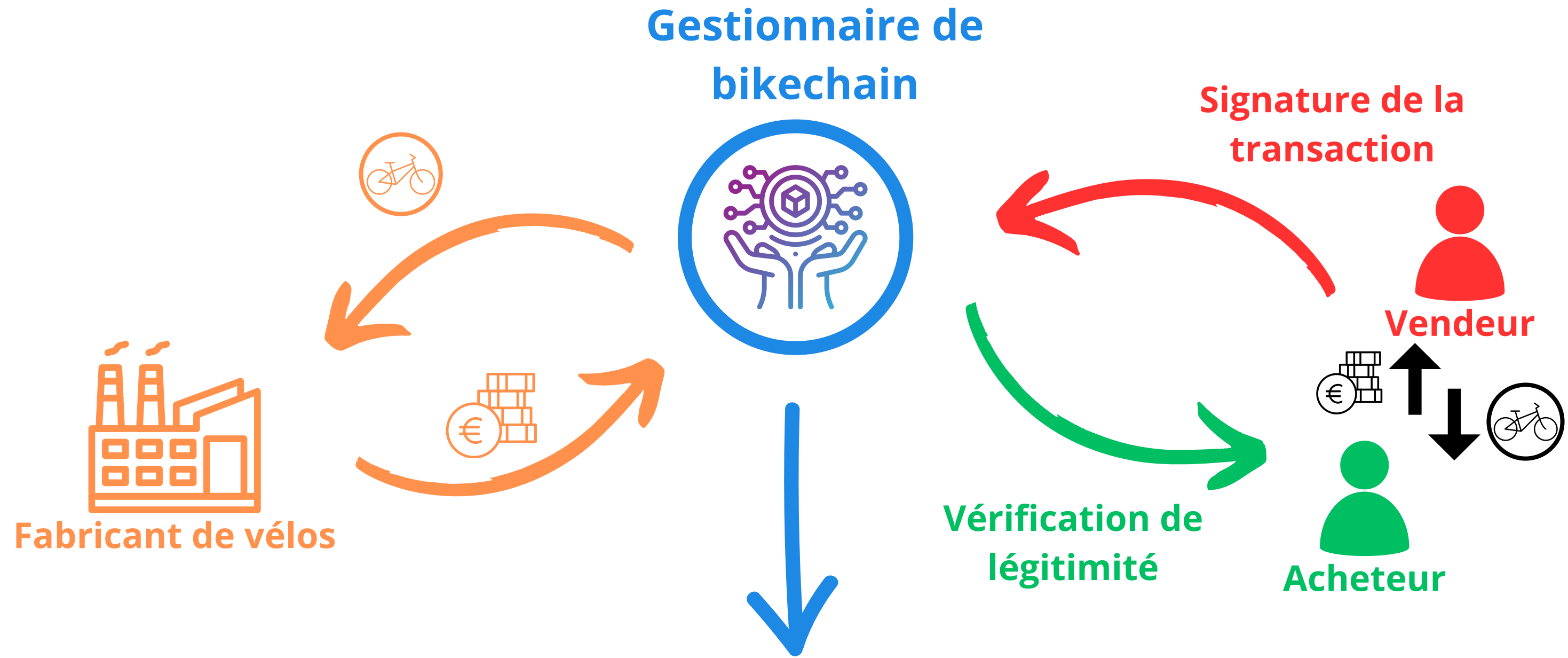
**Acheter des vélos  
d'occasion en toute  
sécurité (signature)**



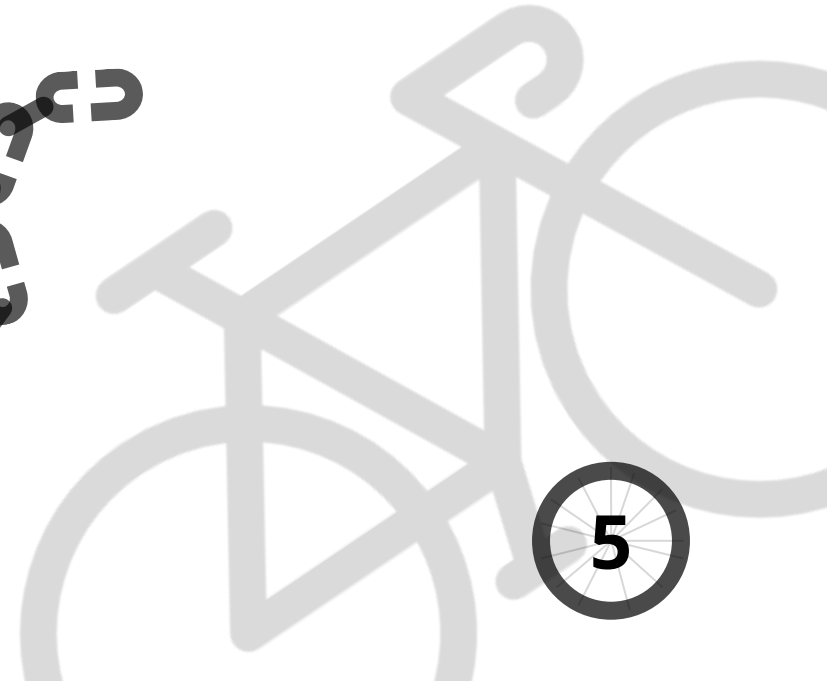
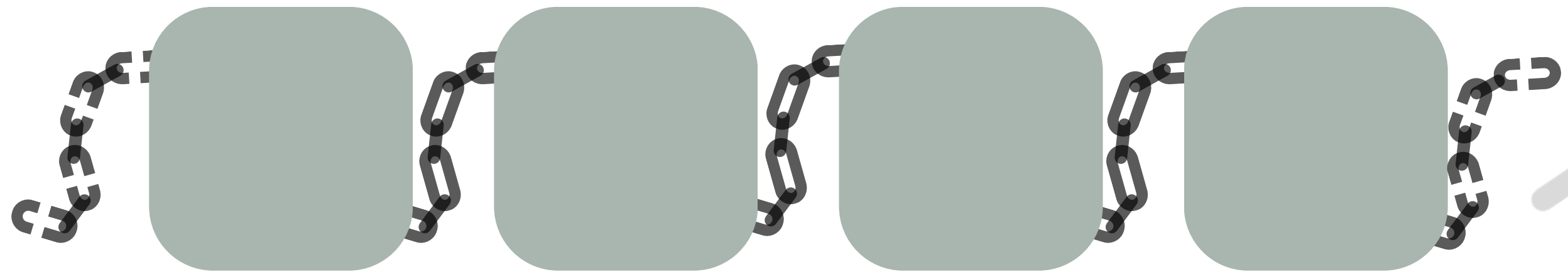


# **LE CONCEPT DE BIKECHAIN**



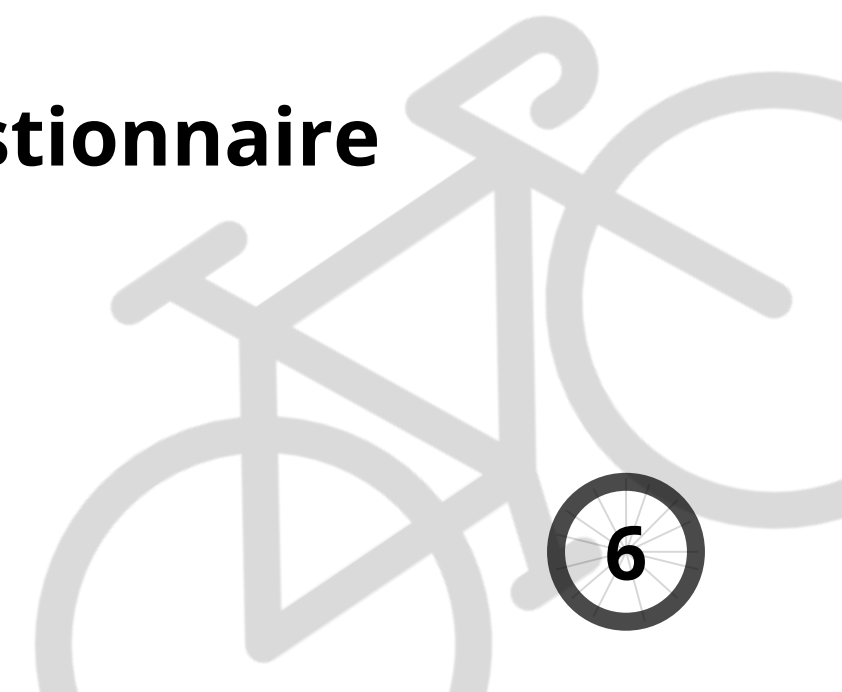
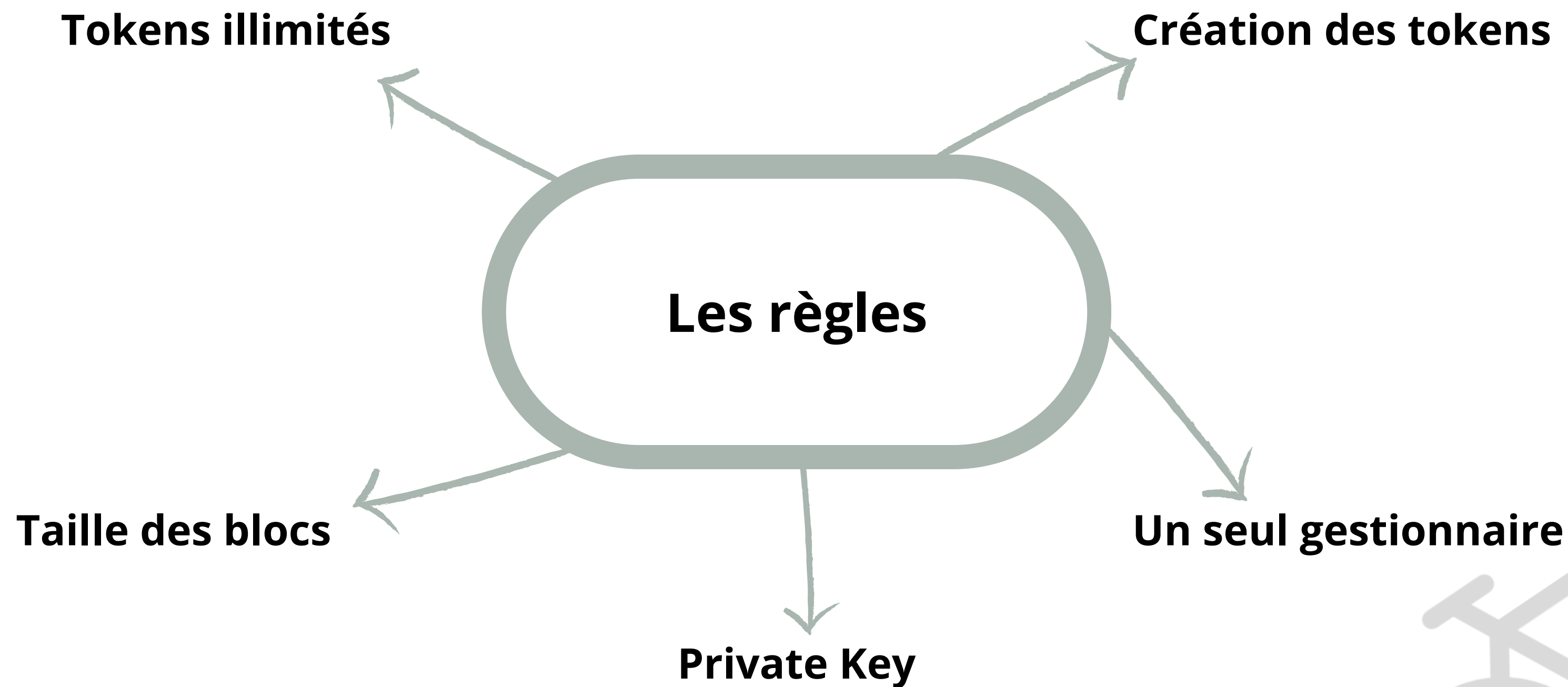


**Enregistrement des transactions dans la blockchain**





# PRINCIPE DE FONCTIONNEMENT





# PREMIERS PAS : VERS LE MVP

## CREATION D'UNE TRANSACTION

Génère une **private key**

Génère une **public key**

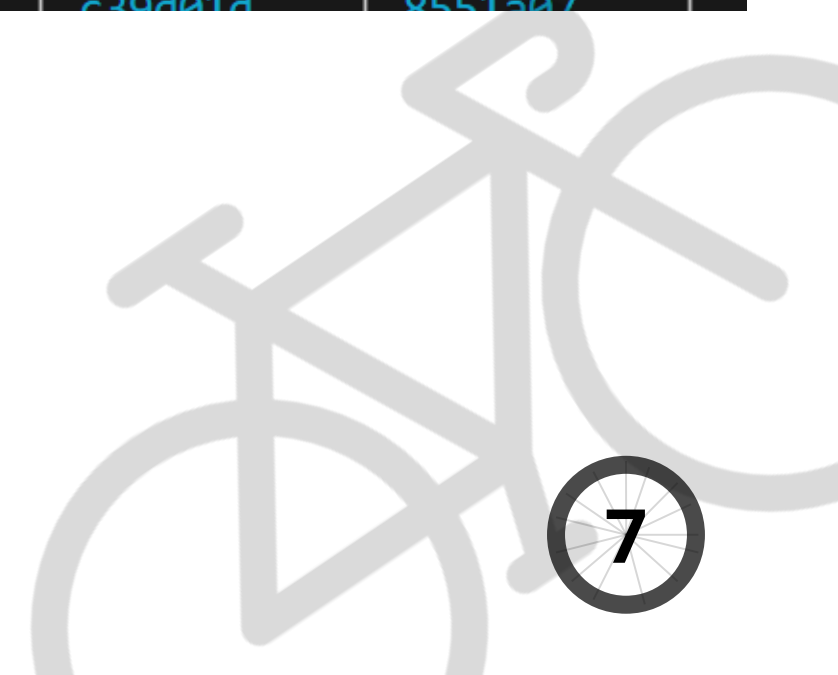
**Ajout manuel de la transaction**

Génère **Date & Heure**

Génère **Hash**

**SIGNATURE** EN PRENANT EN  
COMPTE **TOUS CES ELEMENTS**  
AVEC LA **CLÉ PRIVÉE**

List of transactions				
Hash	Message	Date	Signature	Author
a1fe48346cb100...	Message 0	2023-12-01 08:53:31	f290882...	8551a07...
a310305dbe1434...	Message 1	2023-12-01 08:53:31	de73718...	8551a07...
a081aba0314380...	Message 2	2023-12-01 08:53:31	d5e130c...	8551a07...
c4eaff94464a6d...	Message 3	2023-12-01 08:53:31	06daf1a...	8551a07...
73011f61d0457c...	Message 4	2023-12-01 08:53:31	fb7d1d4...	8551a07...
782cfbf045139a...	Message 5	2023-12-01 08:53:31	cb628cf...	8551a07...
ecf6cadfca2eb2...	Message 6	2023-12-01 08:53:31	c39d01d...	8551a07...







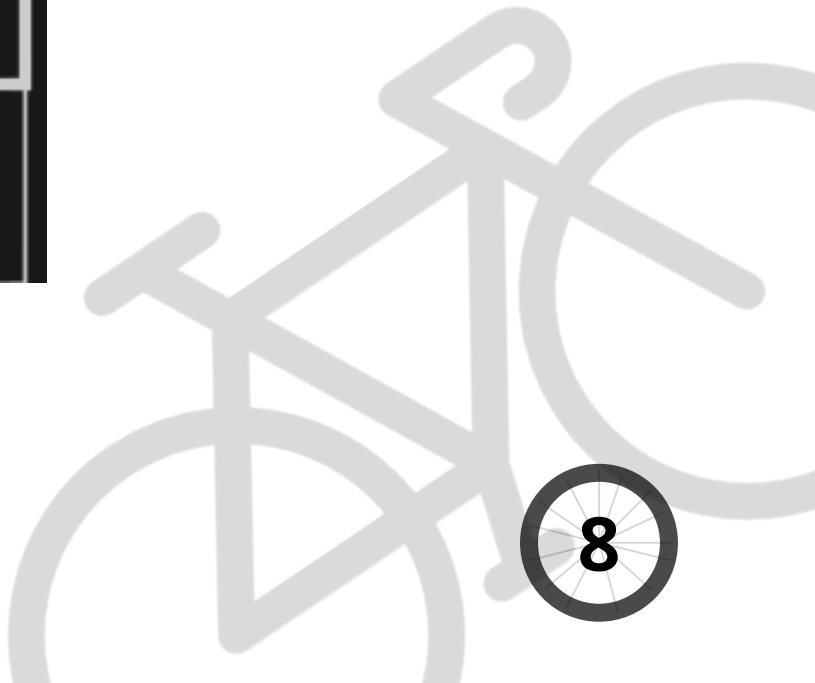
# PREMIERS PAS : VERS LE MVP

## LA STRUCTURE DE LA BLOCKCHAIN

Pour plus de lisibilité, on limite le **nombre de transactions**  
**à 2 par bloc** (arbitraire)

Fonctionnement classique avec fonction “mine”, etc.

Block #2 -- 0005da7...c1235fc -> 0006c1b...71f637e		
Author	Message	Date
8551a07...96624da	Message 2	2023-12-01 08:53:31
8551a07...96624da	Message 3	2023-12-01 08:53:31





# AJOUT DE FONCTIONNALITES

## VERIFICATION DE L'IDENTITE DU VENDEUR

On s'assure que le vendeur **possède bien le vélo**

Block #1 -- 00056eb...36a3a88 -> b8c9afb...2f99dd5		
Author	Message	Date
aae7048...d8c1553	{'serialNo': 'd841a71024597087bd135cecb0554b604384abd5c5240b4...' 'hashPublicKeyBuyer': 'eb37f1450724370b86cdeea5ec328efca0b7bf9c7d0749d...'	2023-12-01 09:06:04





# AJOUT DE FONCTIONNALITES

## PROTECTION DE L'IDENTITE DU VENDEUR

Le numéro serial du vélo est hasher pour ne pas savoir publiquement qui possède le vélo

Block #1 -- 00056eb...36a3a88 -> b8c9afb...2f99dd5		
Author	Message	Date
aae7048...d8c1553	<pre>{'serialNo': 'd841a71024597087bd135cecb0554b604384abd5c5240b4... 'hashPublicKeyBuyer': 'eb37f1450724370b86cdeea5ec328efca0b7bf9c7d0749d...</pre>	2023-12-01 09:06:04





# AJOUT DE FONCTIONNALITES

## INTERFACE



	Index	Previous Hash	Proof	Timestamp	Transactions
1		b8c9afbcffade82b1a3682a742f6b641cc5	2472	2023-12-01 10:08:38.908007	
2		000293820c198f2aed3edf55d0a4c095f9a	8327	2023-12-01 10:09:04.592893	\{"author":\ "4e2427f82c15301962361b3





# **PLACE À LA DÉMONSTRATION**



# EN PRATIQUE



- **Qui devrait être le gestionnaire de la blockchain ? Pourquoi pas directement les fabricants de vélos?**
- **Pourquoi ne pas faire payer les utilisateurs ?**
- **Le système est-il sécurisé ?**



# AMELIORATIONS FUTURES



- **Scalabilité de la blockchain**
- **Intégrer la blockchain avec un marché de l'occasion en ligne**
- **Étendre le concept à d'autres objets possédant un numéro de série**



**MERCI DE VOTRE ATTENTION**

