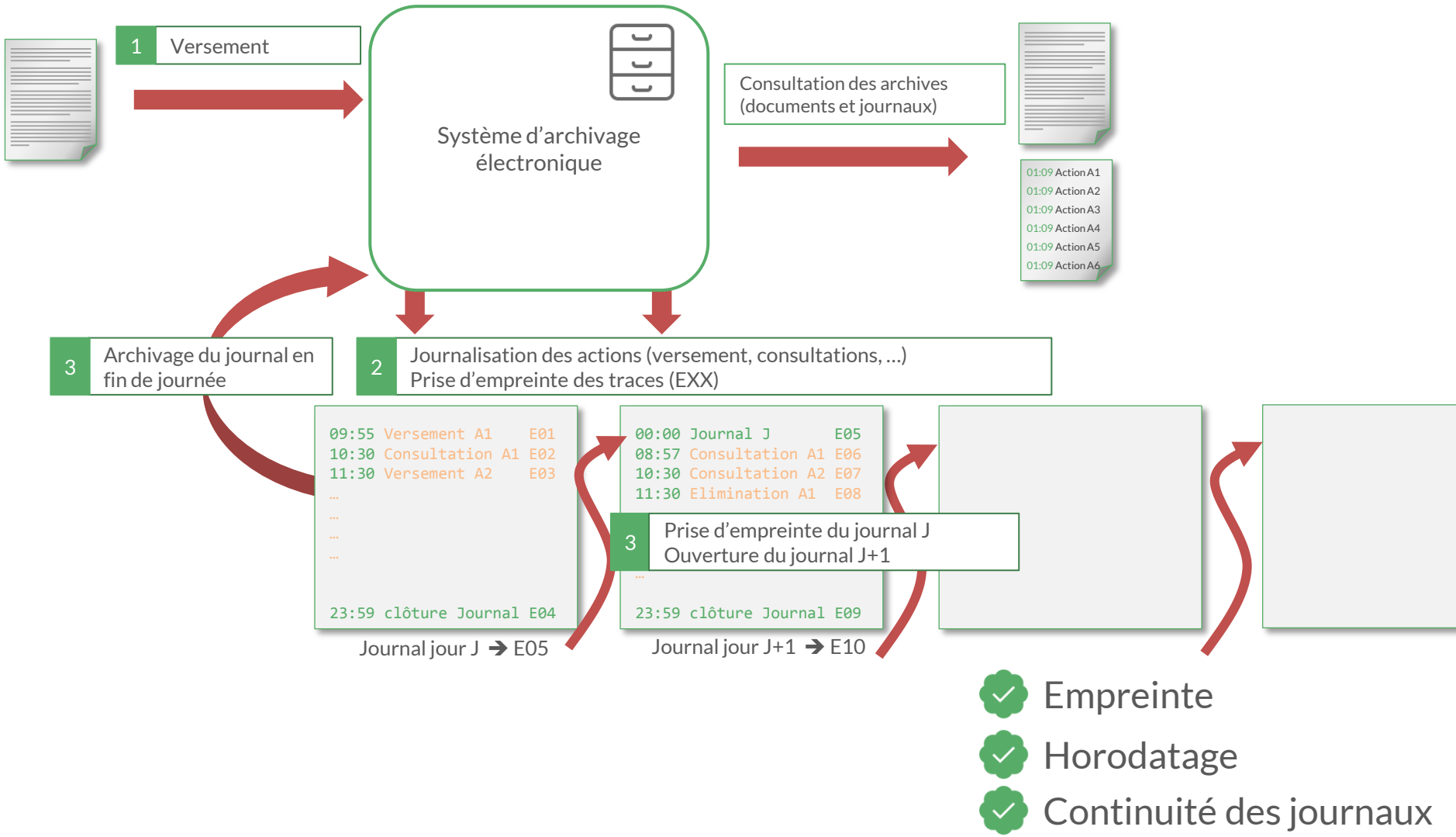
La blockchain des Archivistes

Introduction aux principes de la blockchain

eFutura
28/09/2017

KL

Principes de la journalisation NF Z42-013



KL

Une blockchain se résume à un grand registre dupliqué chez chaque participant d'un réseau et sur lequel on inscrirait tout type d'informations.

Chaque nœud du réseau est chargé de tenir à jour le registre et de vérifier les inscriptions qui y sont faites.

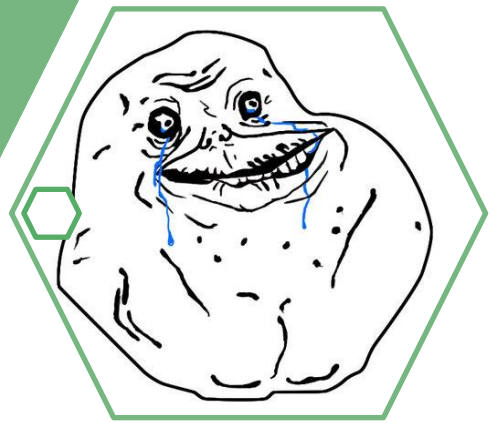
Chaque participant dispose du registre au complet.

Les types de blockchain

Publique

Privée

Consortium



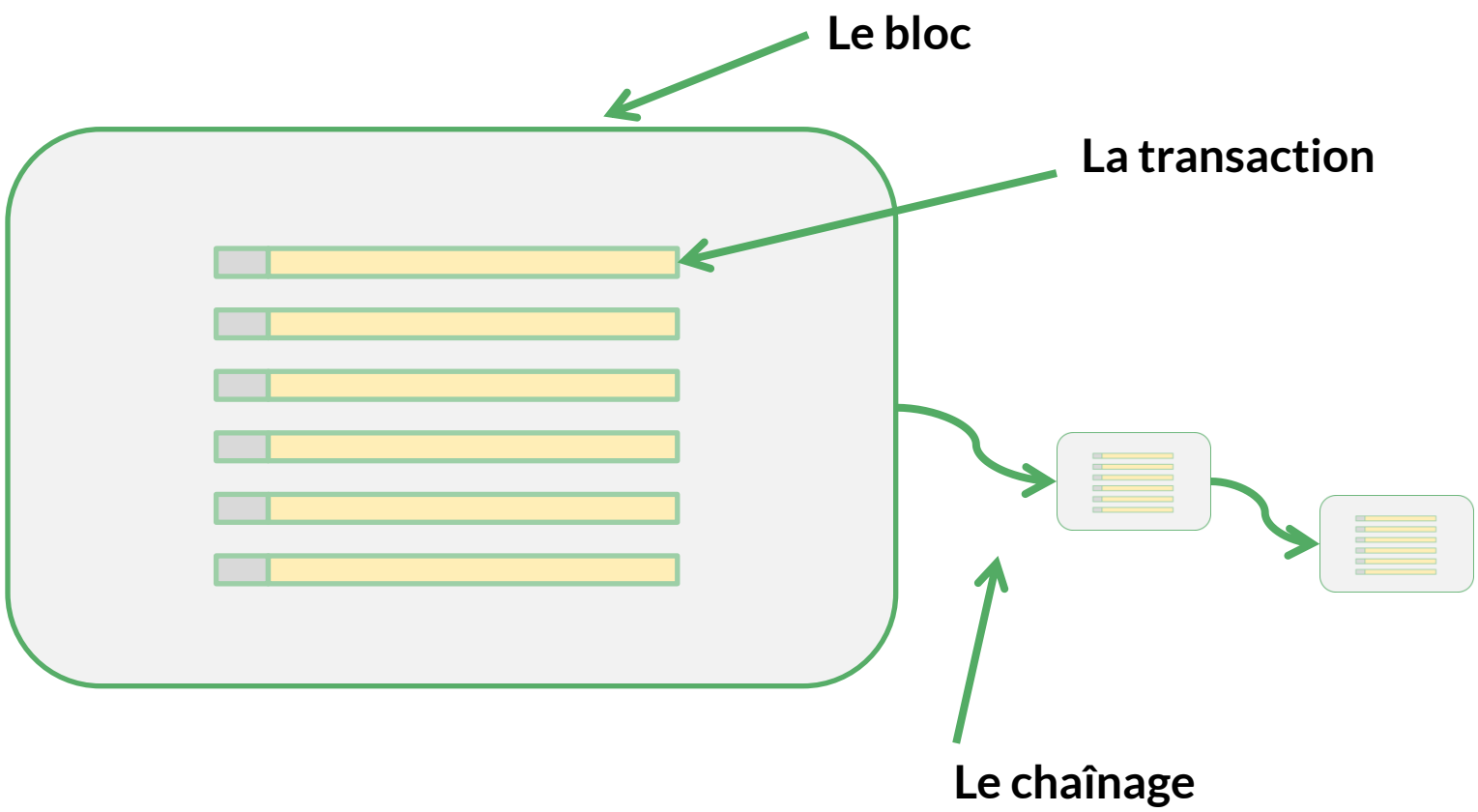
Le monde se construit autour des technologies

Exemples de plateformes :

Caractéristiques	Ethereum	Hyperledger Fabric	R3 Corda
Description	Blockchain générique	Blockchain générique	Blockchain verticale dans le domaine de la finance
Gouvernance	Développeurs	Linux Foundation	R3
Type	Publique ou Consortium	Consortium	Consortium
Consensus	Proof of Work	Variante du Byzantine fault tolerance	Notarisation
Support	*Microsoft*	IBM	R3

Et se cherche encore…

Anatomie de la blockchain



La transaction

- **La transaction** : En informatique, c'est une suite d'opérations qui fait passer d'un état A à un état B
  - C'est l'équivalent d'une ligne dans un registre
  - C'est un contrat entre deux parties sur des termes définis à un instant donné.

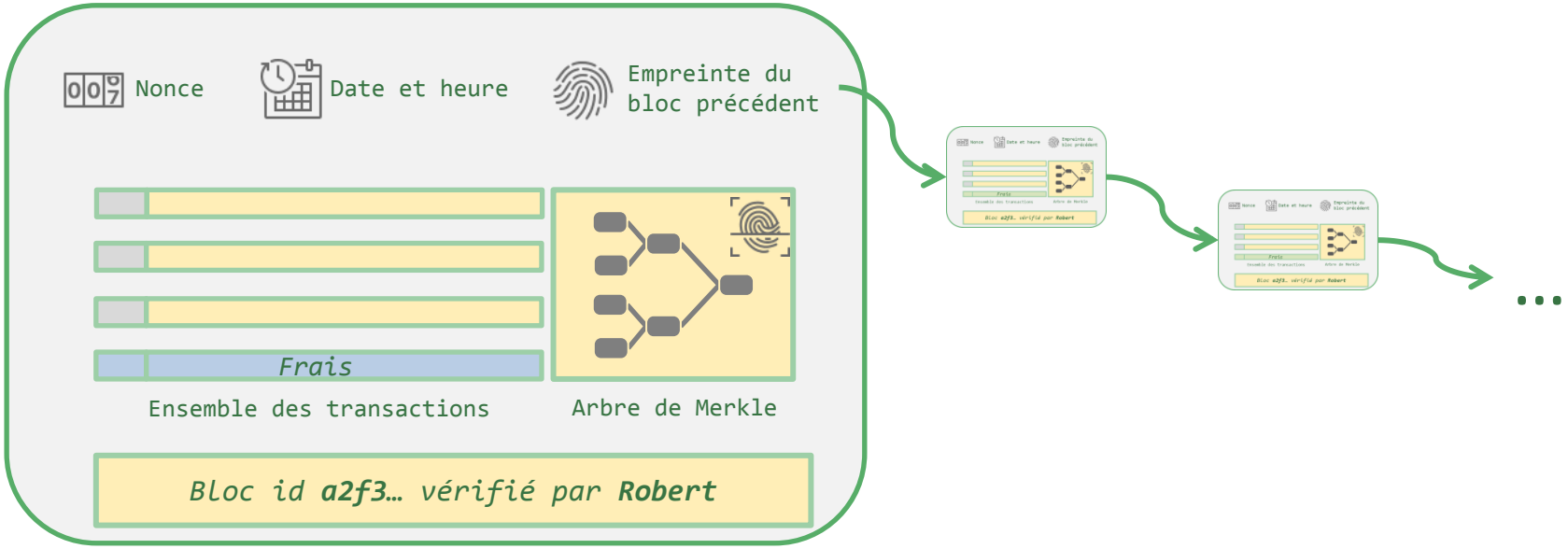
- Problématiques résolues par la signature électronique des transactions :
  - **Authentification** : impossible d'usurper l'identité du signataire
  - **Non-répudiation** : Le signataire ne peut déclarer que la transaction n'a pas eu lieu
  - **Intégrité** : La transaction ne peut être modifiée après coup

De: Bob	**De:** Bob, **À:** Alice, **Quoi:** montre à gousset, **Date:** 01/03/2017 23:33:15.123, **Valeur:** 2, **Frais:** 0.1
	*Transaction signée par **Bob***

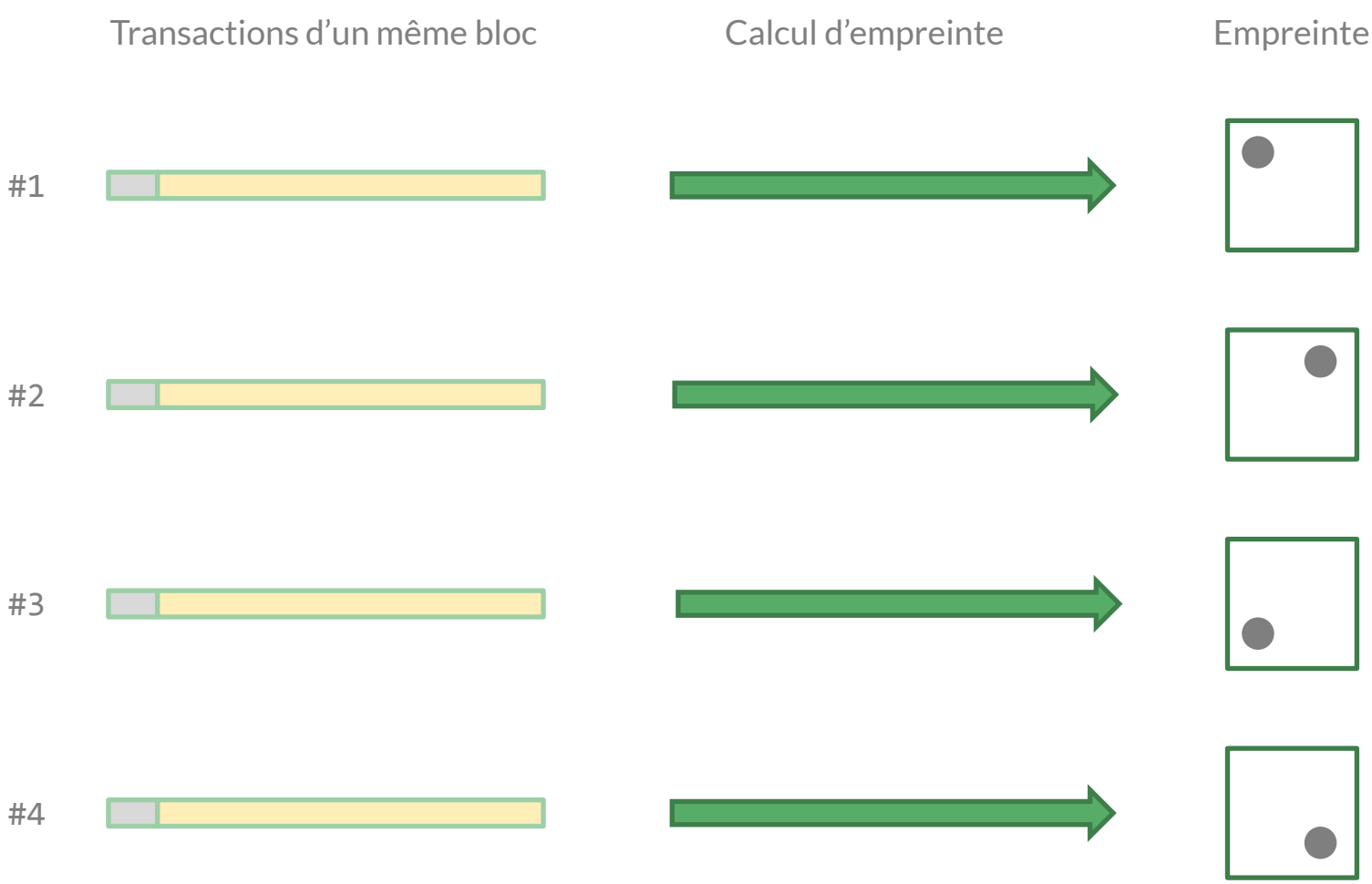
De: Alice	**De:** Alice, **À:** Bob, **Quoi:** montre automatique, **Date:** 15/03/2017 22:30:11.001, **Valeur:** 1, **Frais:** 0.05
	*Transaction signée par **Alice***

Le bloc

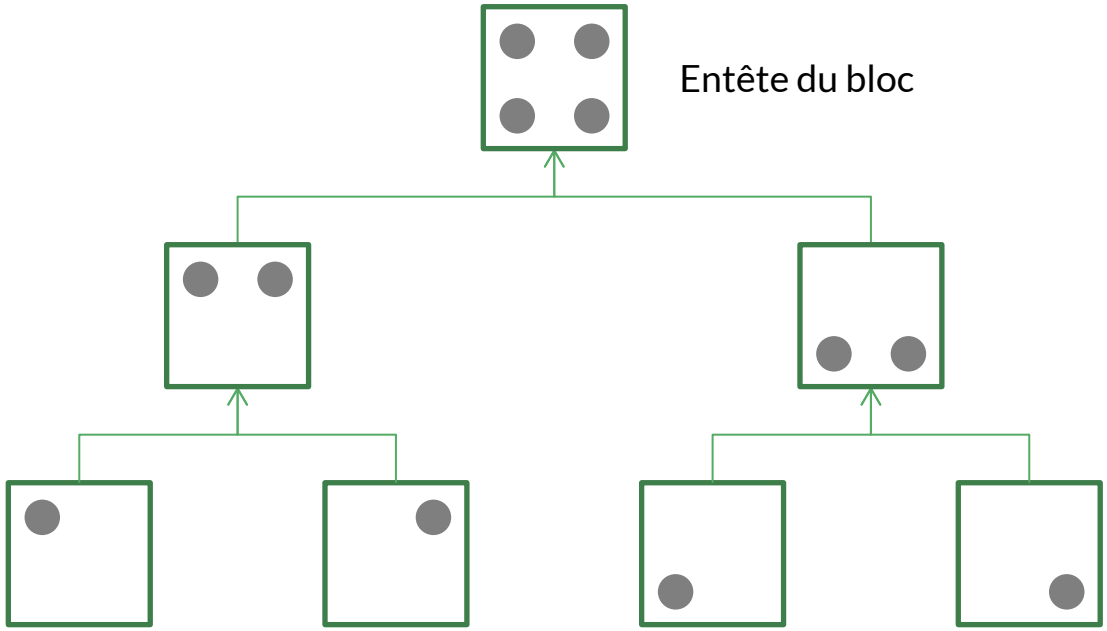
- **Le bloc** : C'est l'équivalent d'une page de registre
  - Il est construit par les nœuds du réseau
  - Il requiert un consensus pour être accepté par le réseau



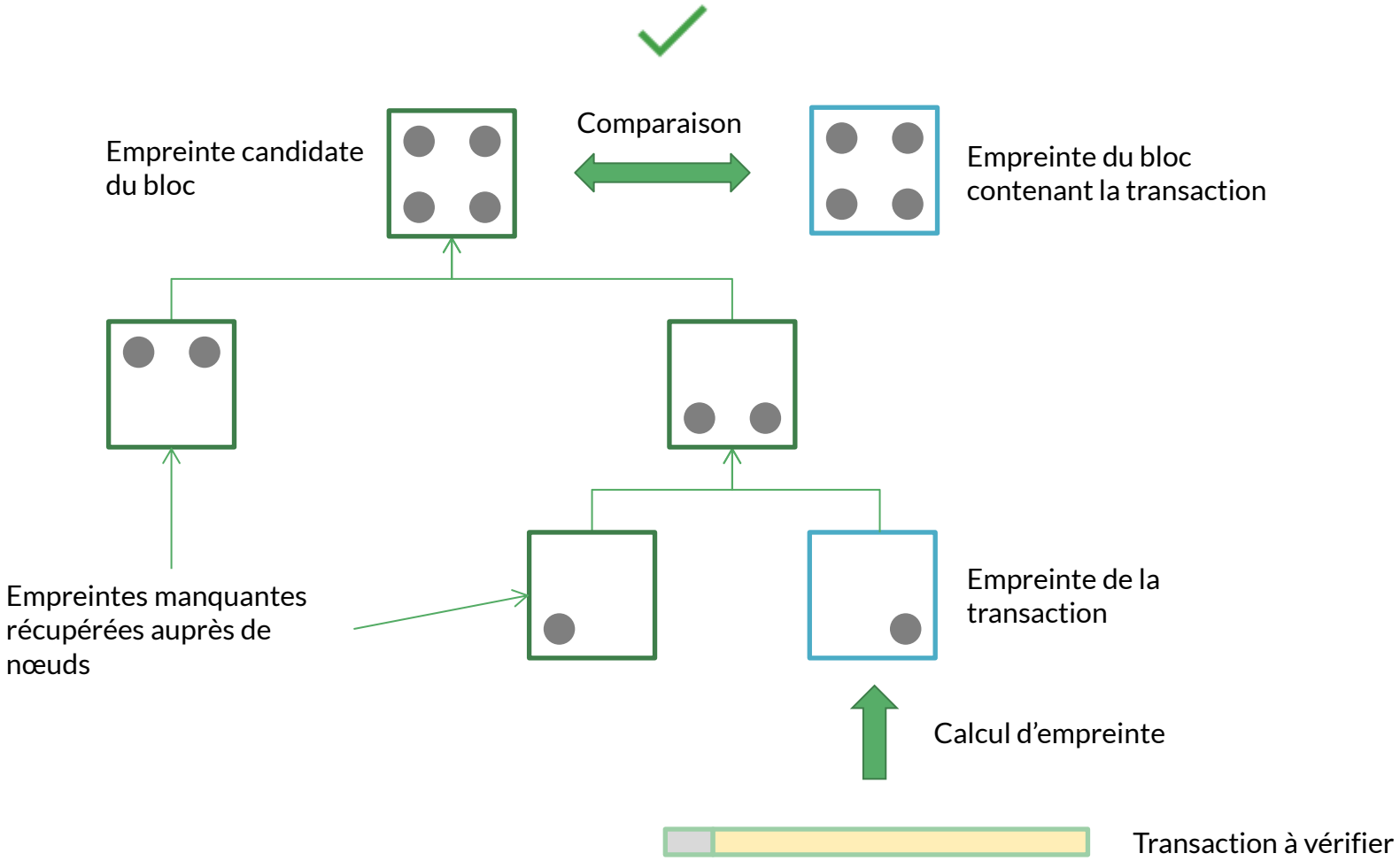
Arbre de Merkle



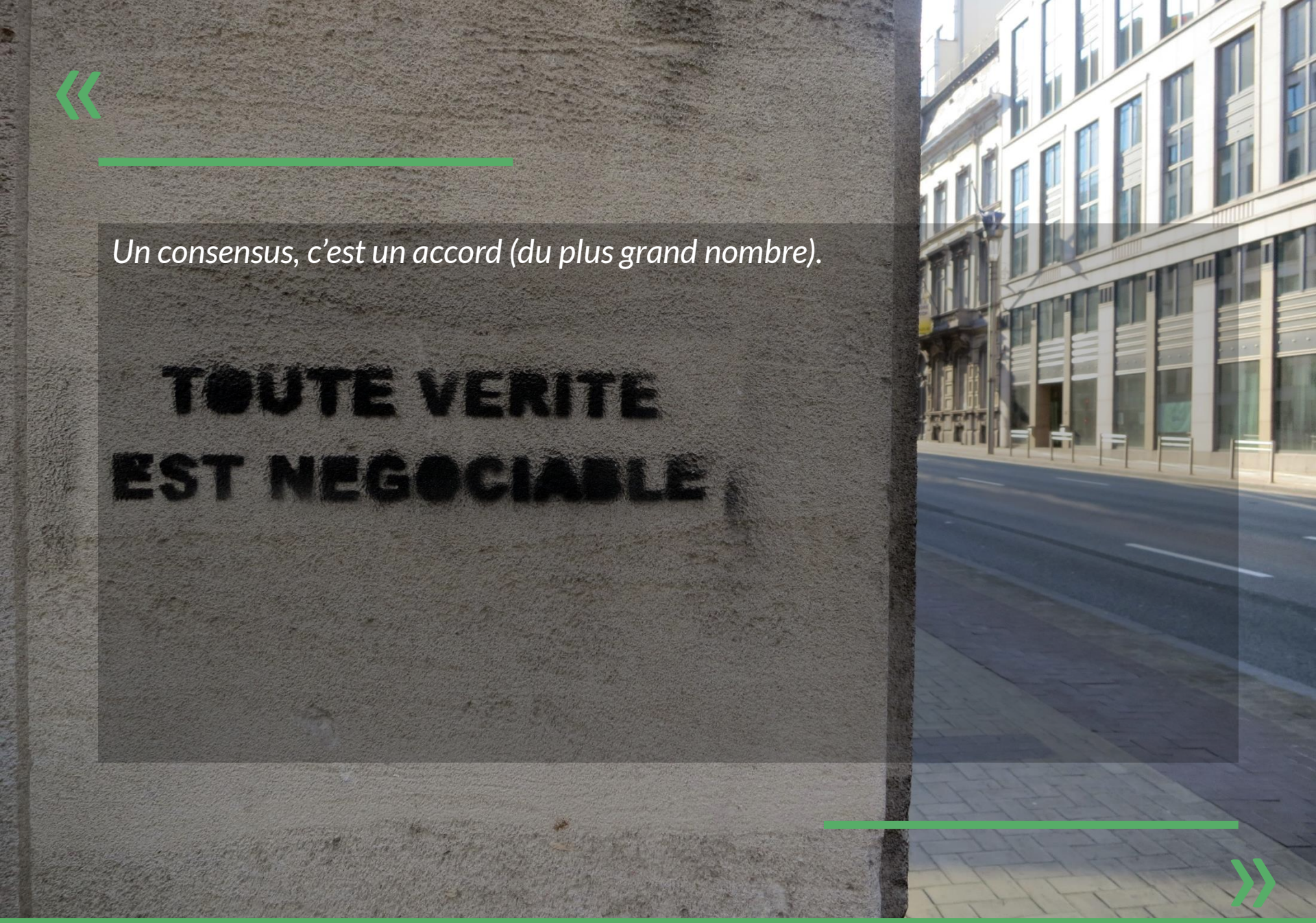
Construction de l'arbre de Merkle



Vérification d'une transaction



Un consensus, c'est un accord (du plus grand nombre).

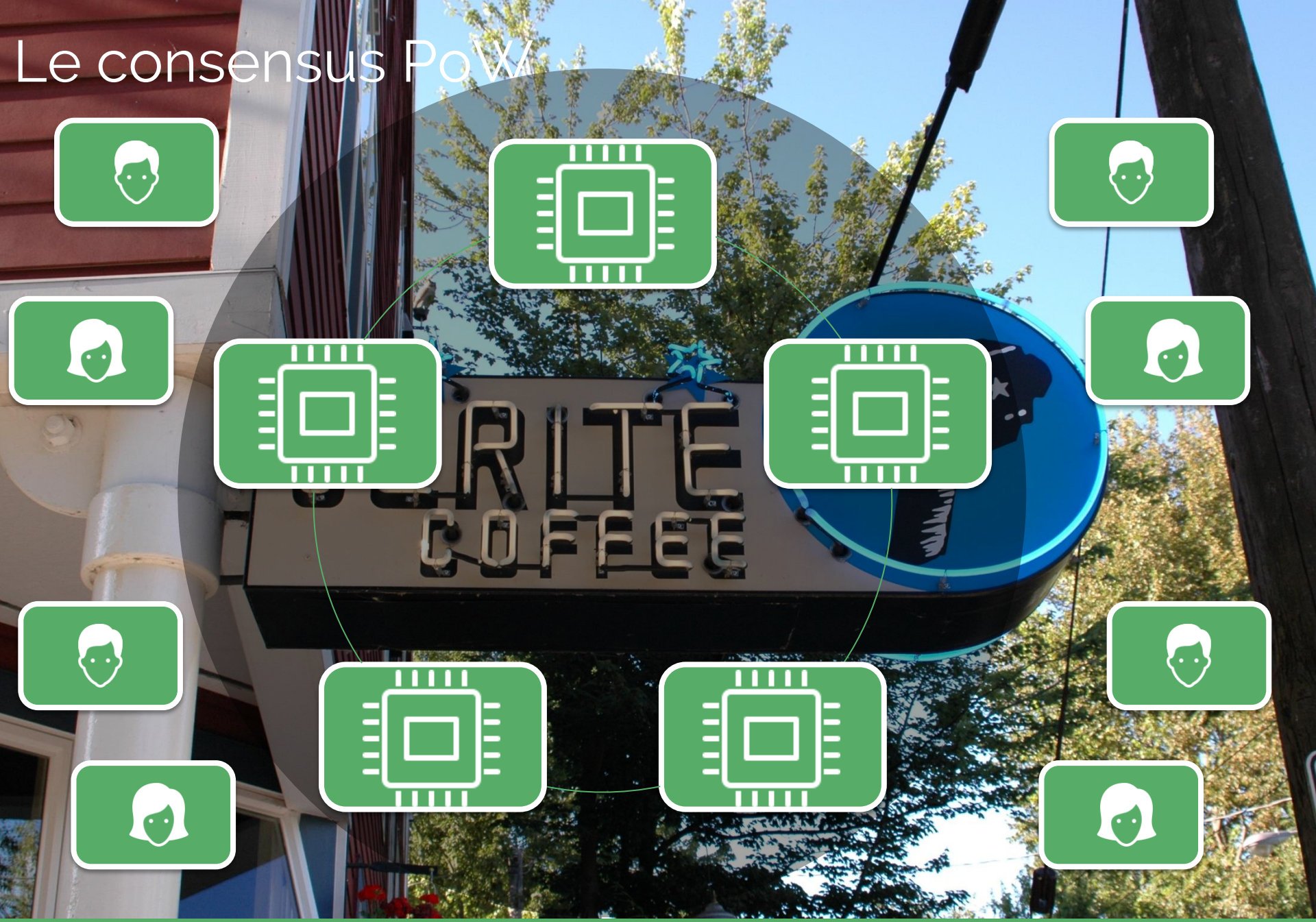


KL

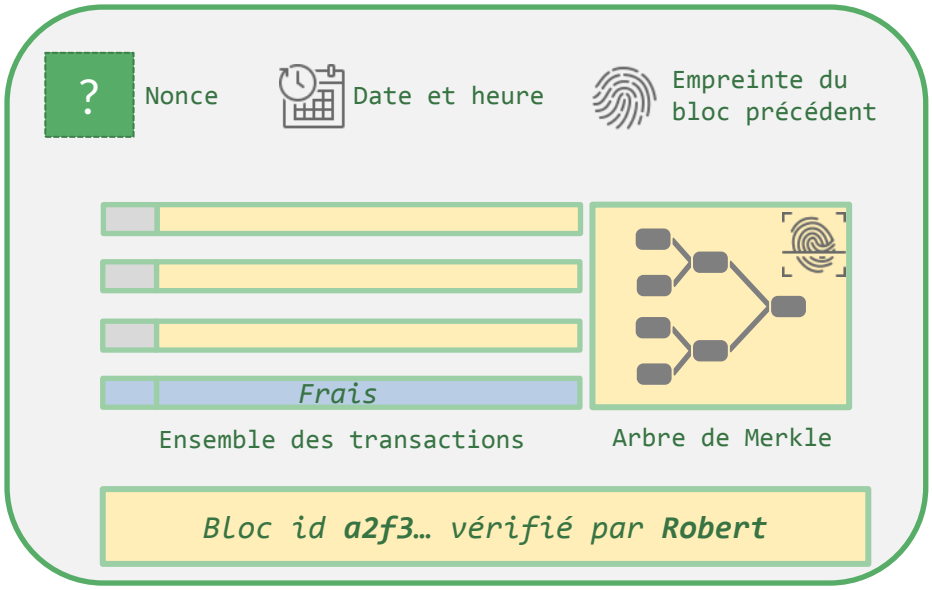
Le consensus

KL

Le consensus PoW



Le consensus Proof of Work



Nonce #00001 → af23d54c3b285…

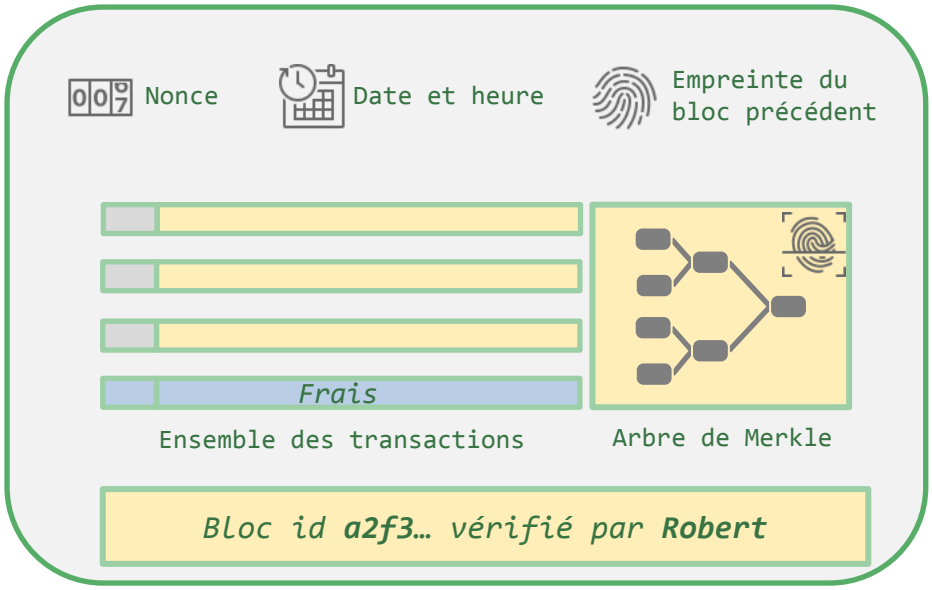
Nonce #00002 → ffff3b4945e43…

Nonce #00003 → 054f3d92c0a582…

Nonce #05432 → 0000005a4f3c63…

Pour Bitcoin, 18 zéros actuellement
Source : https://blockchain.info/fr/home

Le consensus Proof of Work



Différents types de consensus : exemples

- **Le proof of work** : C'est la méthode « bitcoin ». Il consiste à produire un bloc ayant la plus petite empreinte possible.
- **Le proof of stake** : Celui qui a le plus d'enjeux dans la blockchain décide. Pour de la monnaie, il doit posséder une certaine quantité de celle-ci. Il devient un « validateur ».
  - Peercoin, Ethereum en 2018
- **Le proof of activity** : il s'agit d'un mélange de proof of work et de proof of stake. On s'arrêtera quand un certain nombre de signatures de nœuds auront été apposées sur le bloc candidat.
- **Proof of burn** : il s'agit de dépenser de l'argent vers une adresse qui n'existe pas afin d'être sélectionné par le réseau pour miner le bloc.

Et beaucoup d'autres :

- **Proof of capacity**
- **Proof of elapsed time**
- **Byzantine fault tolerance**

etc...

Le minage des bitcoins

Une activité principalement chinoise

Cours du bitcoin au 19/07/2017 : 4000$/bc

Exemple de mine chinoise:

4 050 bitcoins/mois

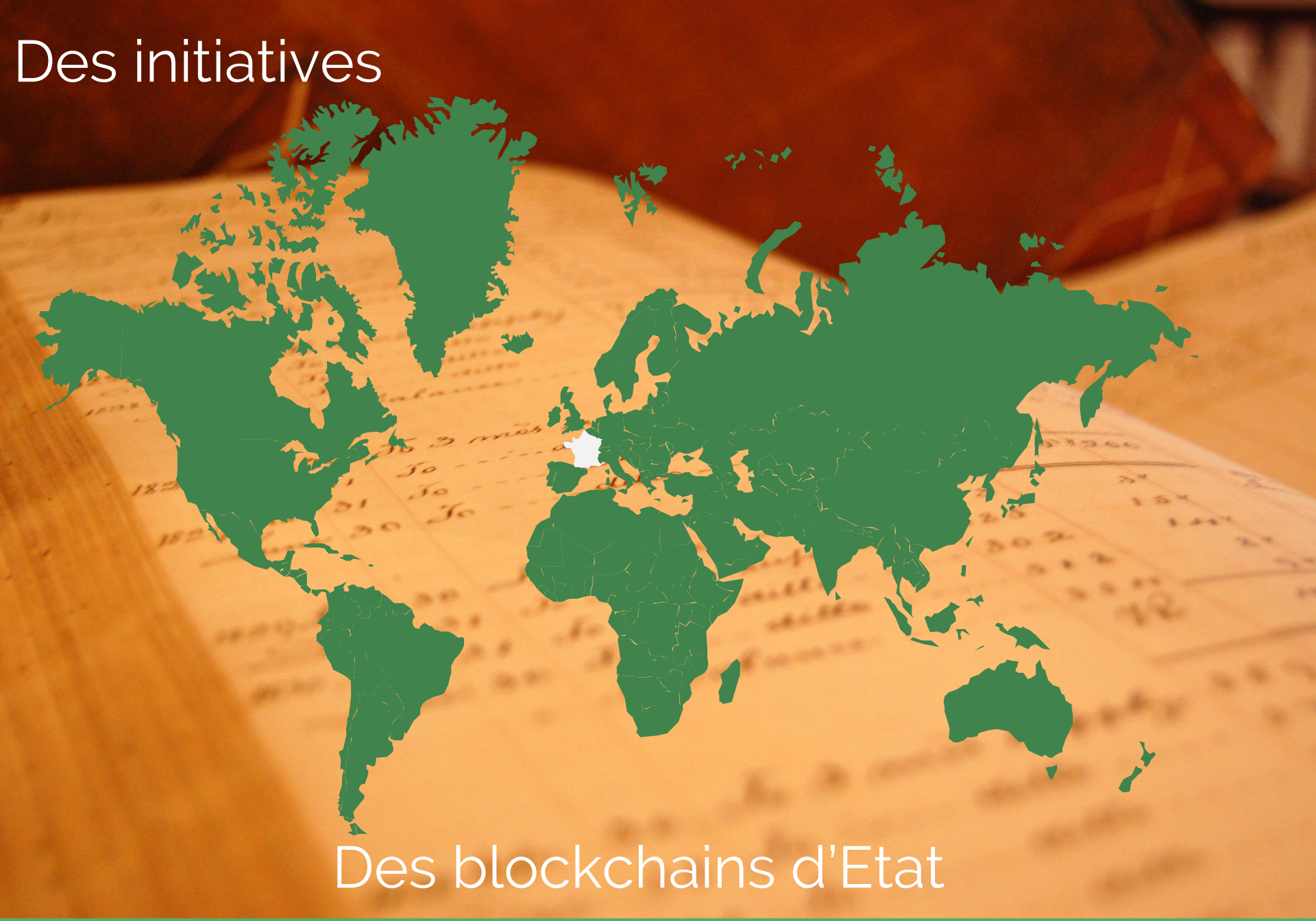
1.5 million de $/mois

4 employés

3% du minage total du réseau

Octobre 2014, source : Motherboard

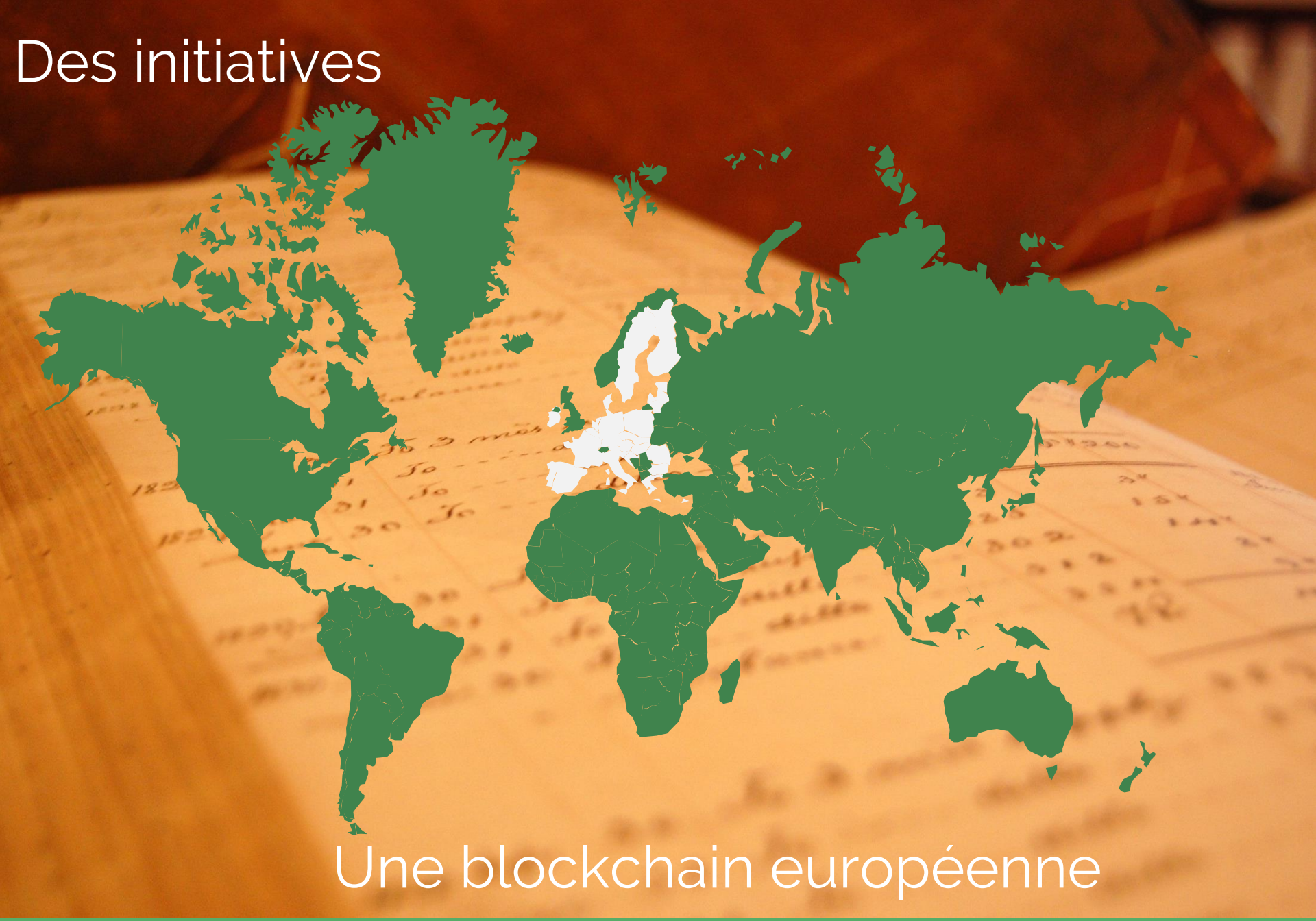
Des initiatives



Des blockchains d'Etat

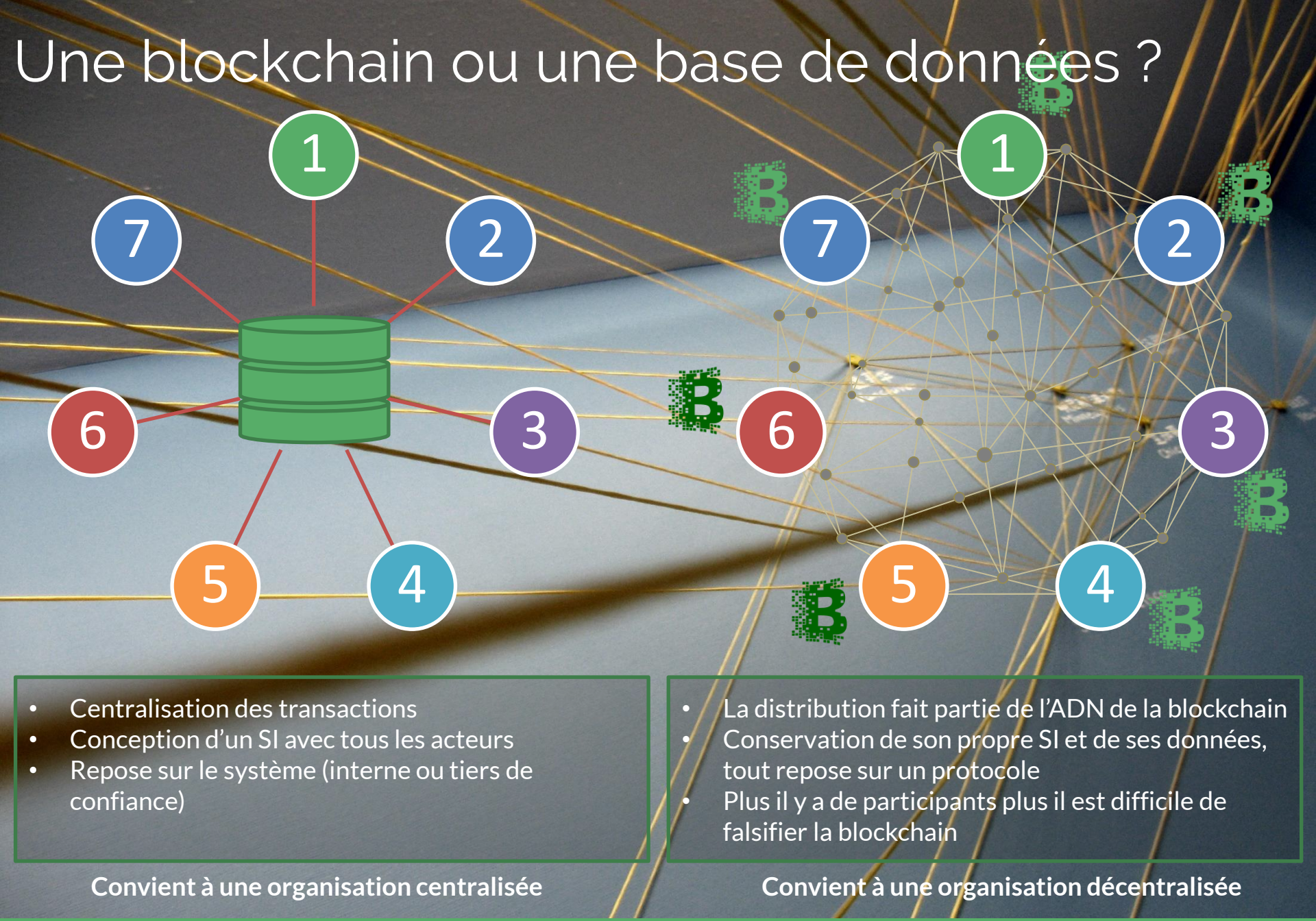
KL

Des initiatives



Une blockchain européenne

Une blockchain ou une base de données ?



- Centralisation des transactions
- Conception d'un SI avec tous les acteurs
- Repose sur le système (interne ou tiers de confiance)

Convient à une organisation centralisée

- La distribution fait partie de l'ADN de la blockchain
- Conservation de son propre SI et de ses données, tout repose sur un protocole
- Plus il y a de participants plus il est difficile de falsifier la blockchain

Convient à une organisation décentralisée

KL

La blockchain des Archivistes

Introduction aux principes de la blockchain

eFutura
28/09/2017

KL

Ressources







Icônes via