CATIE
Solutions pour la société numérique

La blockchain du point de vue technique

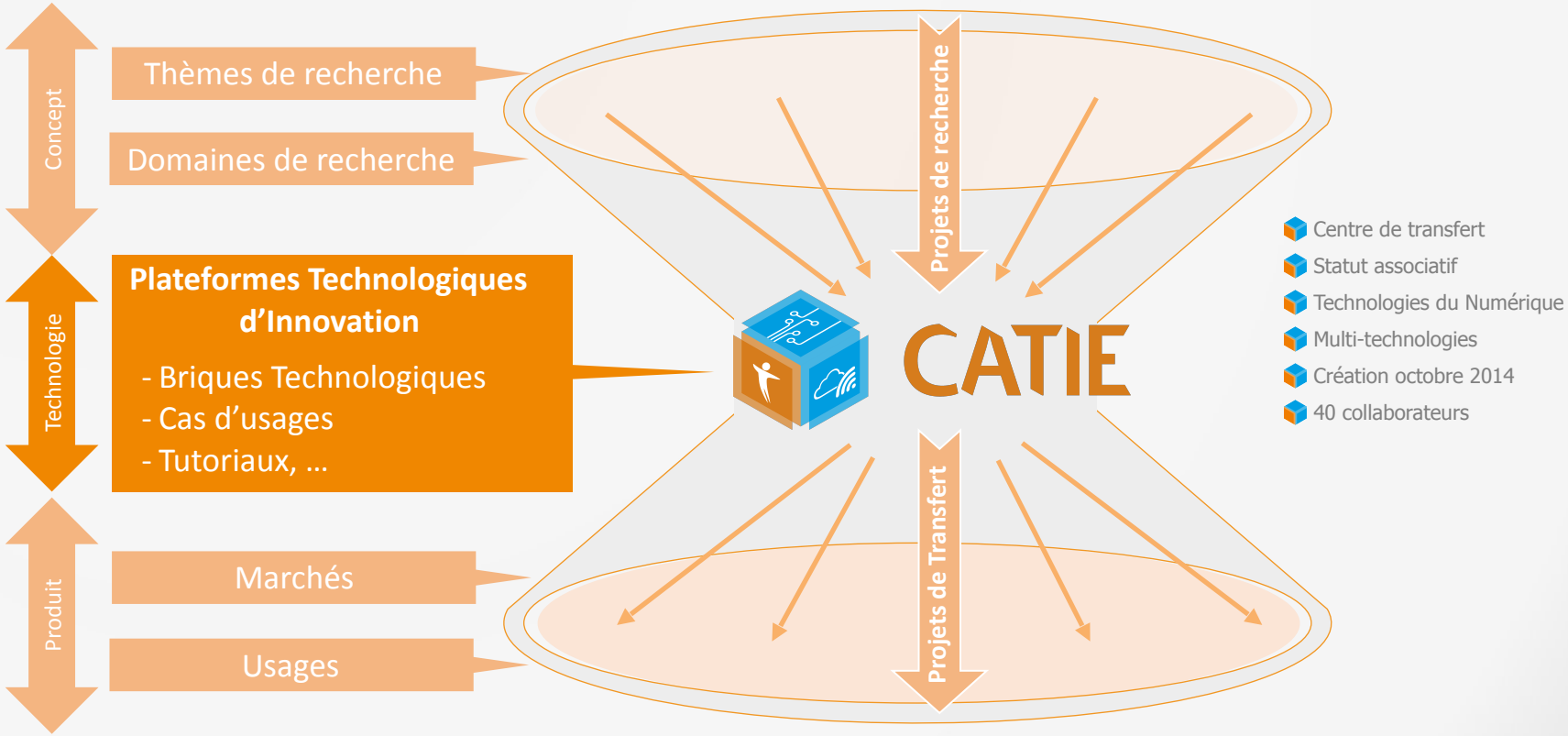
Vinitiques #16, 19 novembre 2019

Charles Garnier, PhD, Ingénieur de recherche
c.garnier@catie.fr

Un centre de transfert technologique

Avec le soutien de la région Nouvelle-Aquitaine

Qui sommes-nous ?



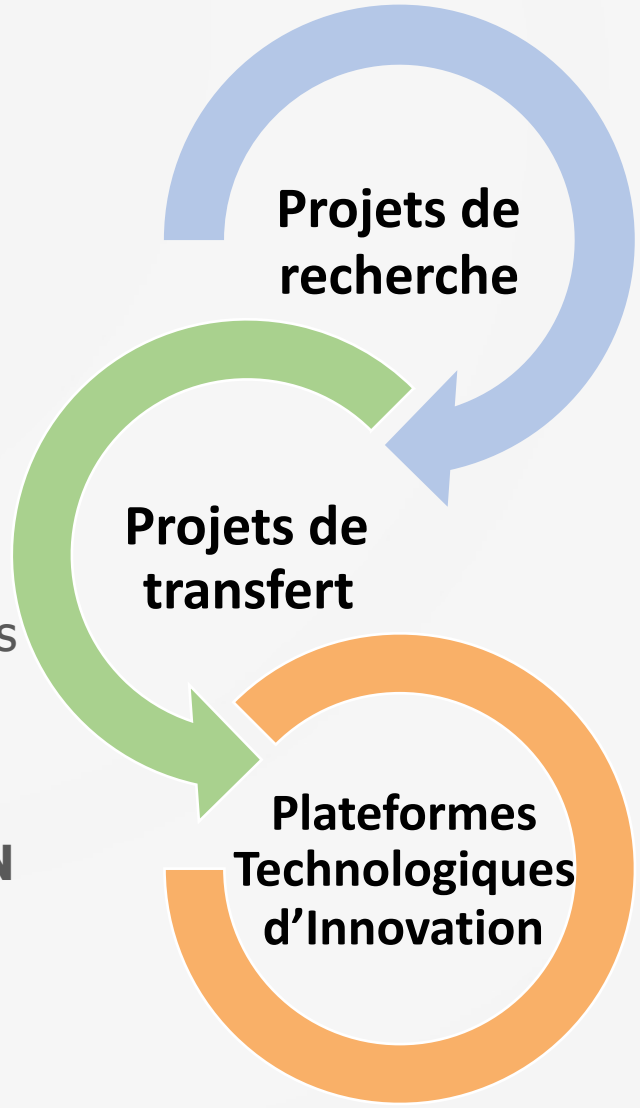
Notre fonctionnement

Qui sommes-nous ?

TECHNO PUSH

- Besoin d'entreprises
- Forte implication CATIE
- Transfert de technologies et de compétences

TRANSFORMATION NUMERIQUE



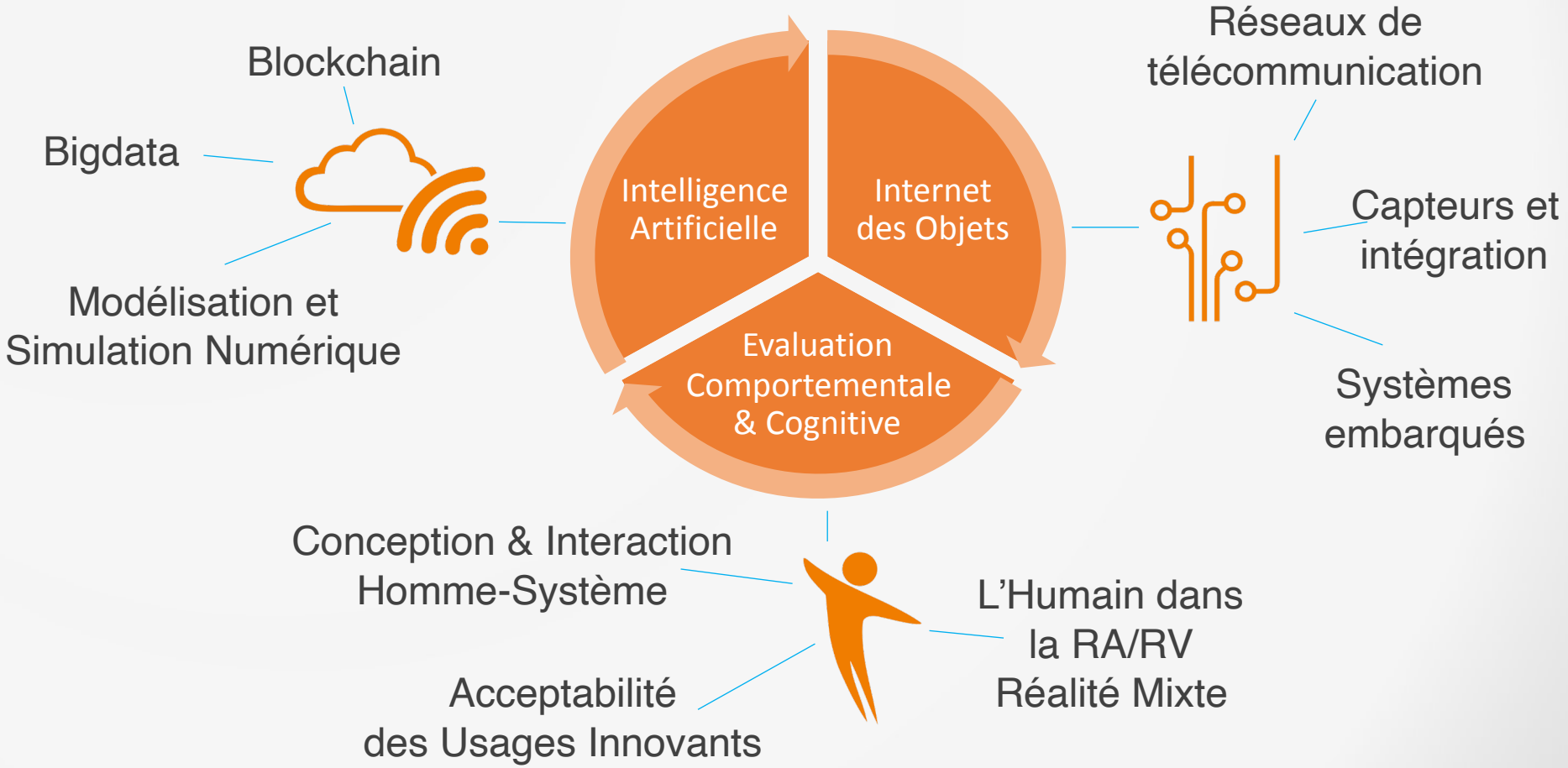
- Menés par des laboratoires
- Participation du CATIE
- Développement de compétences

MARKET PULL

- Intelligence Artificielle : Vaniila By CATIE
- Internet des objets : 6TRON By CATIE
- Évaluation Cognitive & Comportementale : Peac²h By CATIE

Nos thèmes technologiques

Notre organisation



Les promesses de la blockchain

Dans un contexte de crise de confiance, la blockchain promet :

- La **décentralisation** du tiers du confiance,
- Une **confiance distribuée**.

La blockchain promet également :

- Un **système transactionnel**,
- Une **traçabilité** et **non falsification** des transactions,
- Des opérations basées sur des **protocoles complexes**,
- Des **contrats intelligents** s'auto-excécutant.

Les applications

Pourquoi utiliser la blockchain ?

- Diminuer les coûts de traitement,
- Combattre la contrefaçon,
- Remplacer les tiers de confiance,
- Gérer la preuve,
- Réduire les risques de pertes d'informations,
- Gestions des titres de propriétés numériques,
- Traçabilité,
- Système de vote en ligne,
- Plateforme de financement participatif.

Et encore bien d'autres cas d'usages à développer ….

CATIE
Solutions pour la société numérique

La **blockchain** est juste **une écriture comptable d'opérations numériques, partagées entre de multiples d'acteurs.**

Elle ne peut être **mise à jour que par consensus entre une majorité de participants** au système. Et, une fois entrée, l'information ne peut **jamais être écrasée.**

Qu'est ce que la blockchain

Trois piliers principaux

- Dont deux d'ordre technologique :
  - La **cryptographie** asymétrique,
  - Les **systèmes distribués**.
- Et un d'ordre sociologique :
  - Modèle transactionnel dont l'architecture est en mode **peer-to-peer**, offrant la possibilité d'un **consensus distribué** sans nécessité d'un tiers de confiance.

Technologie offrant :

- le stockage et la transmission d'informations : **une base de données / livre de compte / registre**,
- entre personnes individualisées : **utilisant des méthodes d'identification sécurisées et chiffrées**,
- sans intermédiaire défini : **distribuée entre ses participants**,
- transparente : **publique et librement accessible, au moins par ses utilisateurs**,
- sécurisée : **disposant d'un protocole de consensus résistant aux attaques**.

Comment faire consensus ?

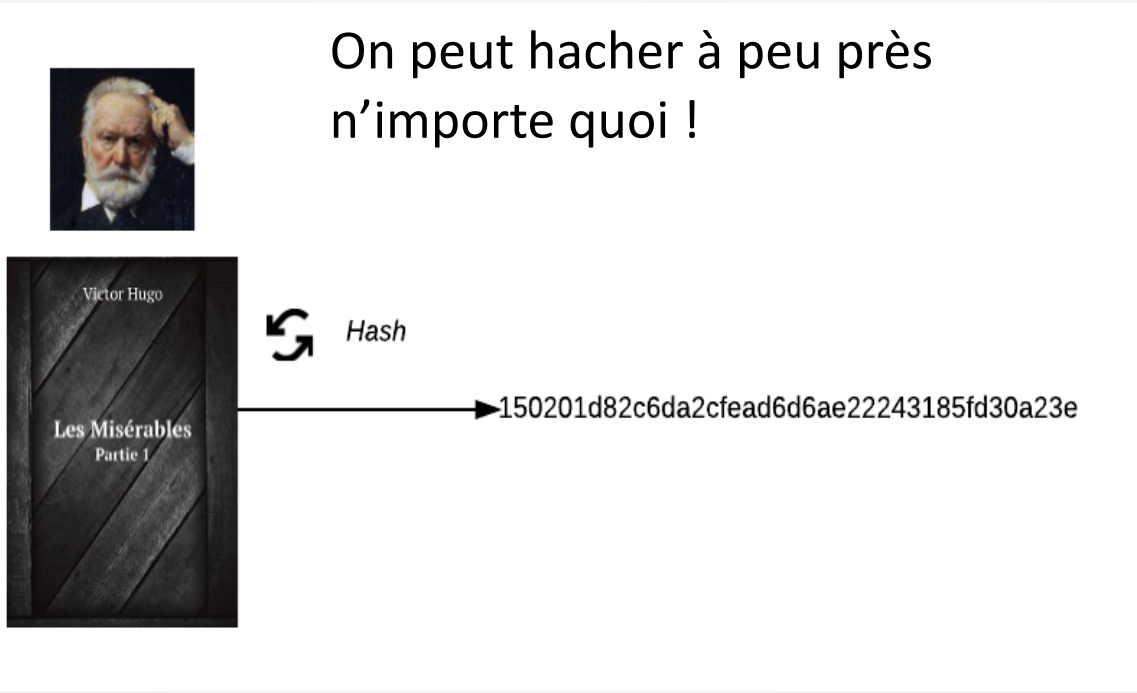
Des transactions possédant une empreinte numérique unique

- **Empreinte digitale** (
  d'une donnée :
  - Rapide,
  - Résistante à la
  - Non réversible

ndensé représentatif

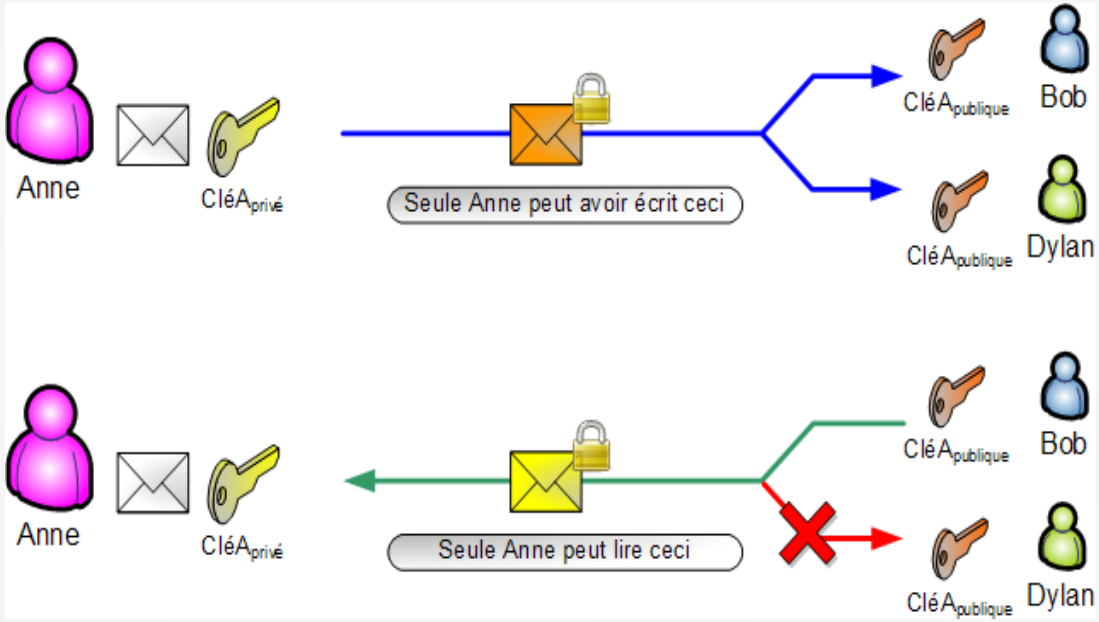
,

Ex : « rapide » = 8cbfb6f1 72b6b3df4ffe26
« rapide ! » = adb954 51afe8e1b259f099



Comment faire consensus ?

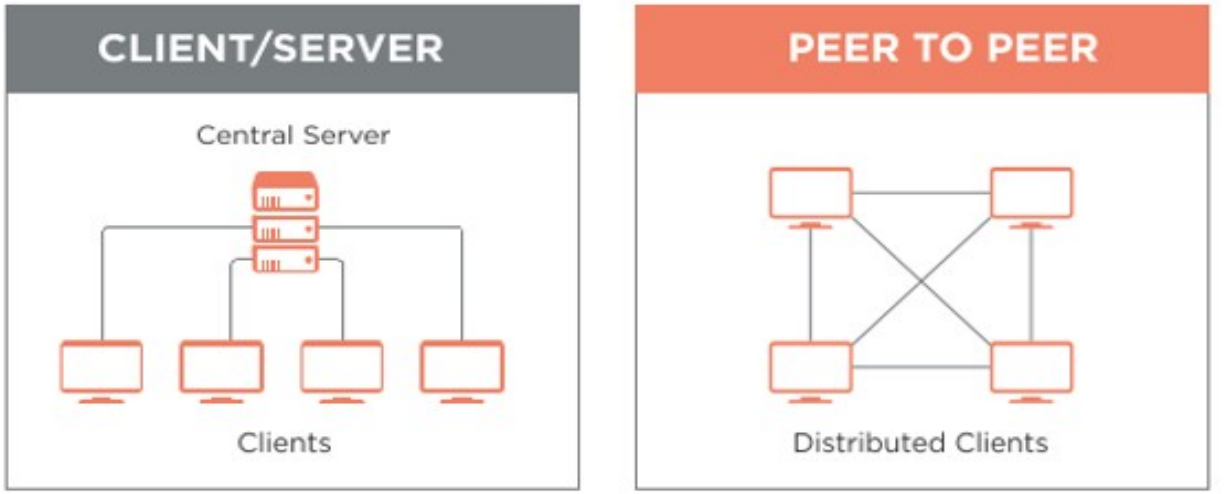
Transmission des transactions entre acteurs de manière cryptée



- **Clé privée** : permet à l'utilisateur d'initier une transaction en signant son message.
- **Clé publique/Adresse** : adresse connue de tous permettant à un émetteur de désigner un destinataire.
- **Signature** = (clé privée + message), unique par rapport au message.
- **Vérification** = décoder la signature avec la clé publique et vérifier que le message est similaire.

Comment faire consensus ?

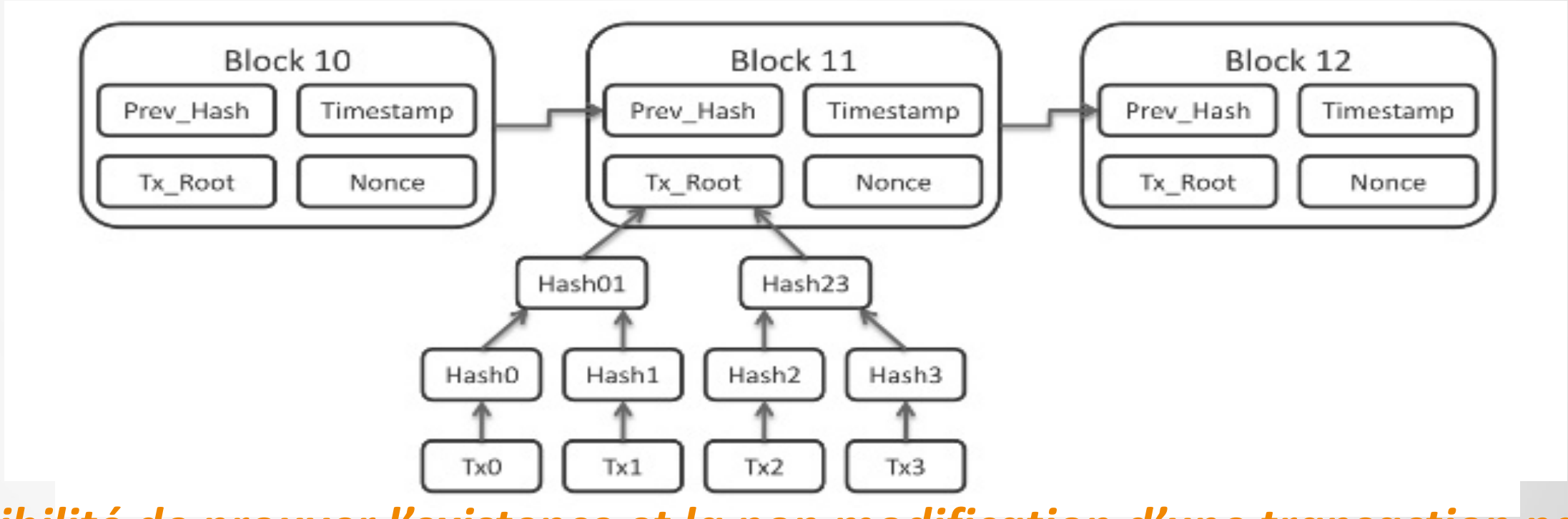
Système distribué



- Protocole **peer-to-peer** : modèle de réseau informatique proche du modèle client-serveur mais où chaque client est aussi un serveur.
- Chaque acteur du réseau à le **même statut, personne ne peut se prévaloir d'une légitimé supérieure**.
- Chaque **acteur possède une copie de l'état** actuel des transactions.

Comment faire consensus ?

Des transactions inaltérables et durables dans le temps : la chaîne de bloc

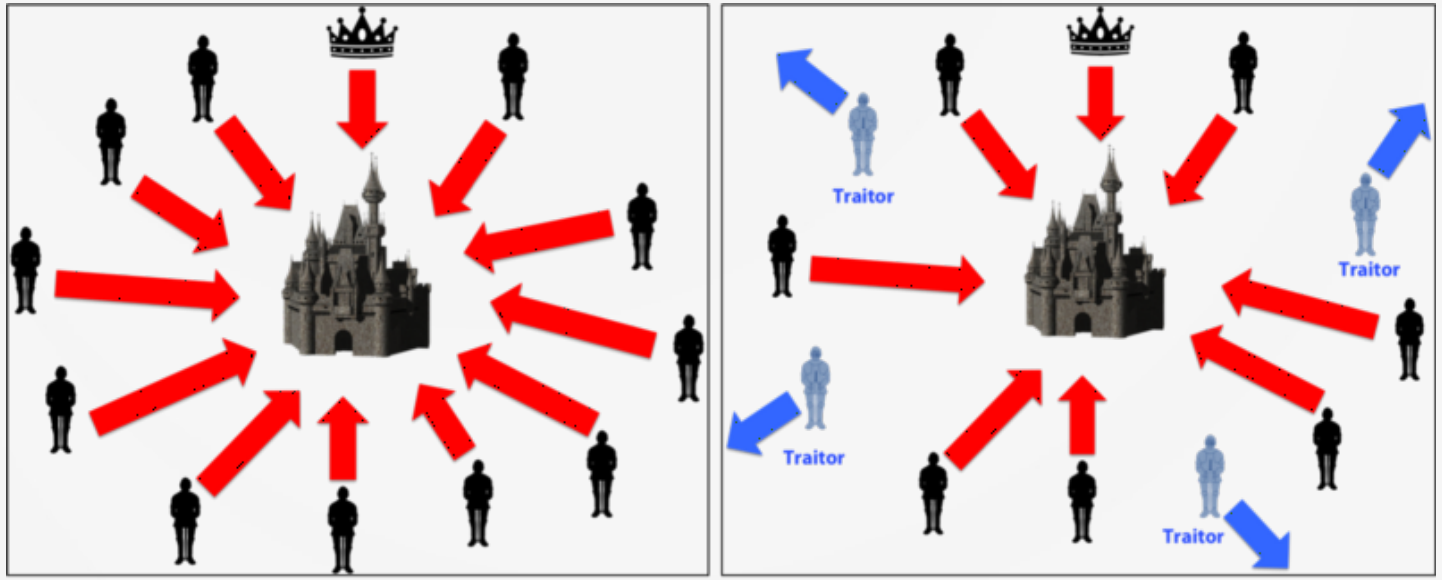


Possibilité de prouver l'existence et la non modification d'une transaction passée

Comment faire consensus ?

Consensus distribué

➢ **Comment apporter une solution au problème « des généraux byzantins » ?**



Coordinated Attack Leading to Victory **Uncoordinated Attack Leading to Defeat**

- Communication uniquement par message.
- Présence possible de traîtres communiquant un faux message.
- Le problème est donc de trouver un **algorithme** pour s'assurer que les généraux loyaux arrivent à se mettre d'accord.

Quel mode de gouvernance pour la blockchain ?

Comment faire consensus ?

Consensus distribué : un choix de consensus qui n'est pas anodin !

➢ Suivant l'usage que l'on réalise de la blockchain, le mode de consensus ne sera pas le même et le choix d'un type de blockchain sera réalisé.

- ✓ Connaît-on tous les acteurs du consensus ? Les acteurs doivent-ils être identifiés ?
- ✓ Quel est le nombre d'acteurs du consensus ?
- ✓ Existe-t-il des impératifs en terme de performance ?
- ✓ Doit-il y avoir une finalité au consensus ?

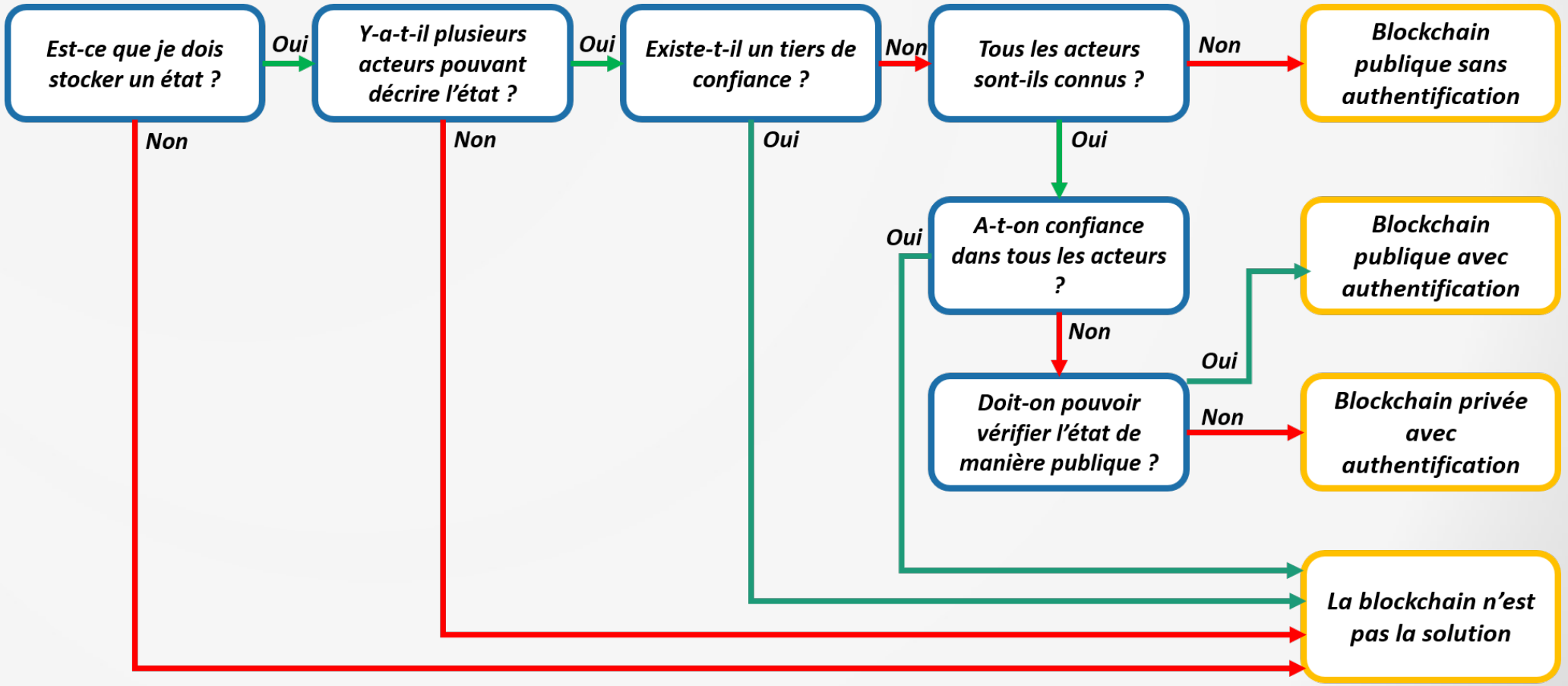
Blockchain publique sans authentification des acteurs :

- Sans restriction à l'entrée : lecture et écriture sur la blockchain ouvertes à tous,
- Sans organe de contrôle et sans prérequis juridiques.

Blockchain hybride/privée avec authentification des acteurs :

- Accès à la blockchain restreint à certains utilisateurs sélectionnés par une organisation centrale,
- Droit de lire la blockchain publique ou restreint à certains utilisateurs.

La blockchain fait-elle tout le temps sens ?



Source : Do you need a blockchain ?, Wüst and Gervais

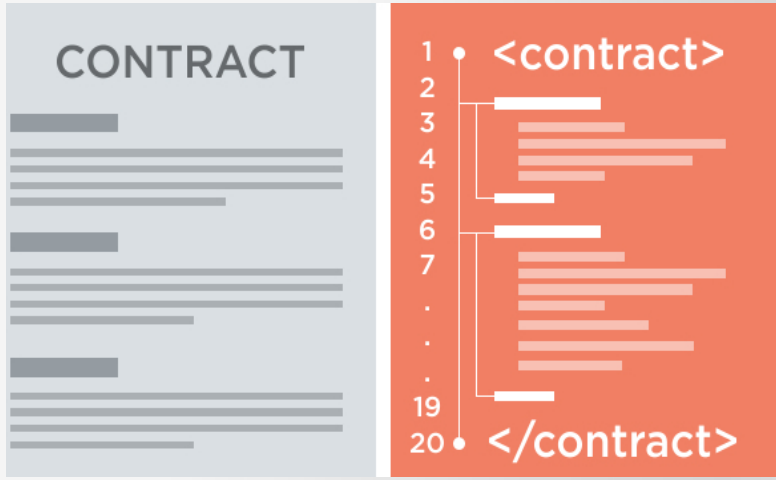
Des contrats vraiment intelligents ?

Notion de « smart contract »

Programmes autonomes associé à un identifiant/compte unique qui exécutent automatiquement les conditions et termes d'un contrat, sans nécessiter d'intervention humaine une fois démarrés. Un simple programme qui est **stocké dans la blockchain et capable de modifier l'état de la blockchain**.

Caractéristiques du « smart contract »

- Turing complet : permet d'implémenter tous les algorithmes de calcul, des instructions de conditions et de boucle, mémoire et stack infinie.
- Le code d'un smart contract est immutable et durable.
- Parle avec d'autres smart contracts,
- Est atomique,
- S'exécute de manière séquentielle,
- Est durable.



Ce que ne fait pas un « smart contract »

Un contrat ne peut pas avoir d'interaction et d'accès directs avec les données du monde extérieur.

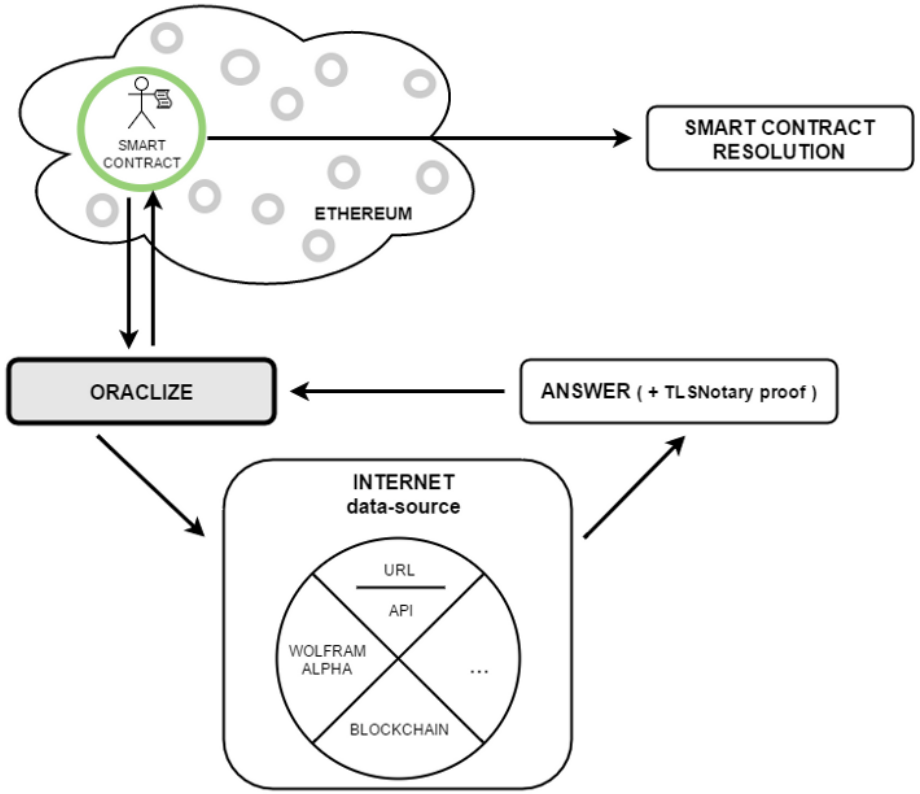
- Ex : interaction avec service web pour récupérer une donnée d'entrée d'un contrat

Le principe des oracles

L'oracle éclaire la blockchain de son savoir

- Service chargé d'**entrer manuellement une donnée extérieure dans la blockchain**,
- Qui va **récupérer l'information** qui lui a été demandée et **l'insère dans la blockchain** à l'endroit qui lui a été assigné.

- Qui est cet oracle ?
- Comment lui faire confiance ?
- Réintroduction d'un tiers de confiance dans une technologie qu'on vante comme *trustless* ?
- Que se passe-il si l'information n'est pas ajoutée par l'oracle, ou si elle est fausse ?



CATIE
Solutions pour la société numérique

Des questions ?

Vinitiques #16, 19 novembre 2019

Charles Garnier, PhD, Ingénieur de recherche
c.garnier@catie.fr

RÉGION Nouvelle-Aquitaine