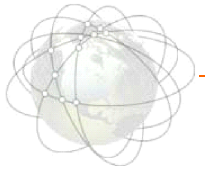


Blockchains *(fr. Chaînes de blocs)*

Principes et fondamentaux

Présenté par **Dr. Samia GAMOURA-CHEHBI**

maj 2017

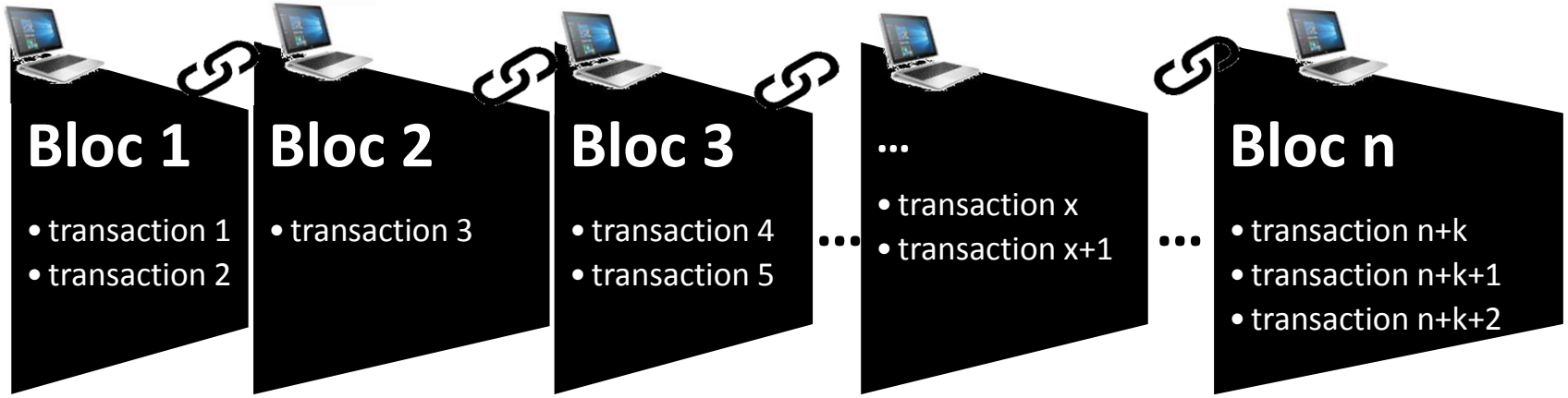
Plan

1. Blockchain … Quoi ?
2. Principe
3. Fonctionnement
4. Scénario
5. Cas d'applications qui existent … déjà !
6. Objectif
7. Potentiel applicatif ?

1. Blockchain : Quoi ?

Une technique collaborative et distribuée de :

- **Communication** (transmissions des informations, échanges et transactions),
- **Stockage** (stockage distribué sur plusieurs postes d'utilisateurs)
- **Sécurisation** des données (cryptage et authentification)



Apport du blockchain par rapport aux systèmes existants

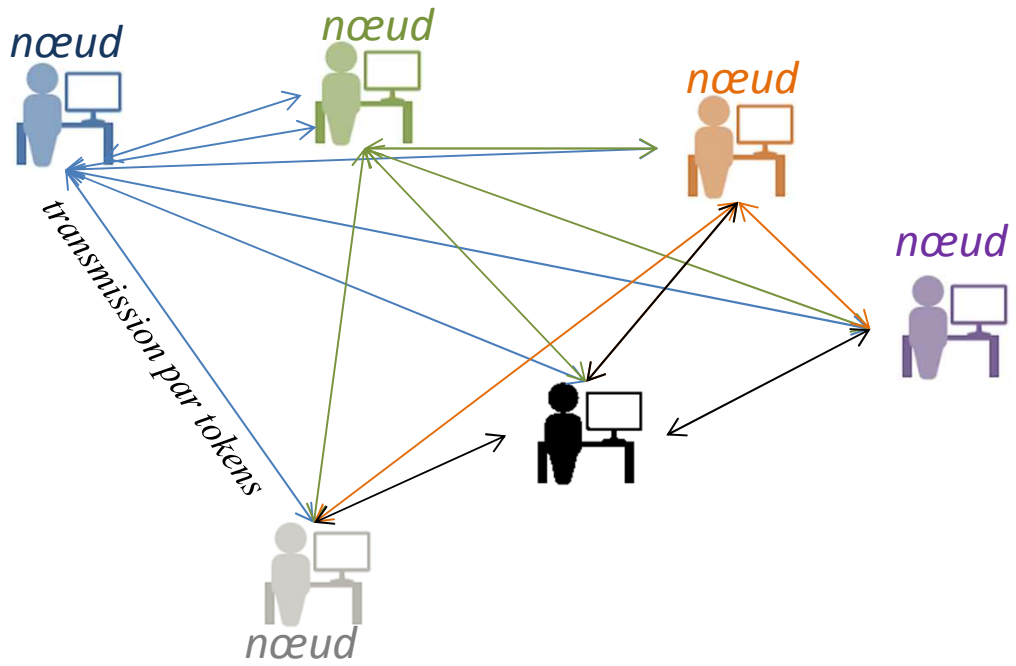
- **Transparence** (réseau ouvert aux participants),
- **Sécurité** (pas d'intrusion puisque approbation demandée par tous)
- **Automatisation** (par d'intervention manuelle ou contrôle)
- **Confiance généralisée** (transactions faites par confiance)
- Pas besoin de **tierse-partie** pour valider les transactions (pas besoin d'une autorité)

1. Blockchain : Principe ?

Couplage des deux aspects :

- L'aspect d'**ouverture** (vu par tout le réseau),
- **Sécurité** et **authentifiable** (approbation collective)

- Principe des **tokens** (jetons programmables) qui fait l'**actif programmable**
- L'ensemble des participants (appelés **mineurs**) s'organisent **un réseau de nœuds**.
- Chaque nœud (poste de travail) abrite un ensemble de **transactions** (opérations)



1. Blockchain : Fonctionnement ?

Chaque bloc d'opérations (transactions), passe par les étapes suivantes:

1. doit être **validé** (tamponné)
2. ensuite **horodaté** (date et heure du jour)
3. ensuite **ajouté** à la chaîne
4. ensuite il devient **visible et accessible** par tous les nœuds du réseau

Exemple 1 : Vote en ligne

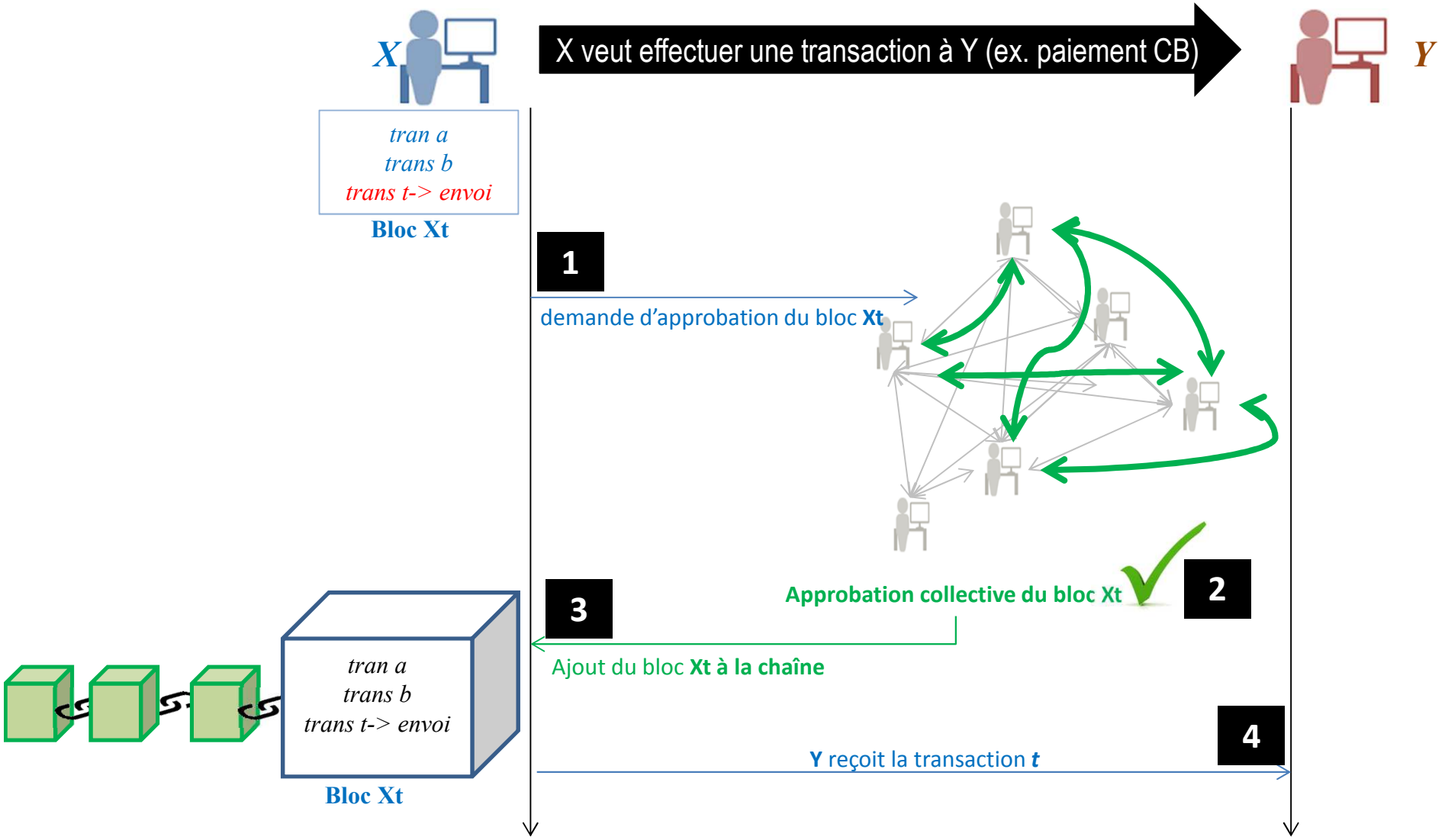
Au moins 3 éléments sont nécessaires pour effectuer un vote sur une blockchain :

1. Un actif programmable,
2. Un protocole (scénario ou processus des opérations)
3. Une clé cryptographique qui permet de s'authentifier par le réseau (ex. sorte de carte électorale qui identifie le votant)

Exemple 2 : contrat intelligent d'assurance de voyage

60 % des passagers assurés contre le retard de leur vol ne revendiquaient jamais leur argent,
A Londre, des développeurs ont mis un système d'assurance de voyage automatisé basé sur un blockchain. Lorsque le vol est en retard, le programme indemnise automatiquement les voyageurs sans l'intervention de l'assureur ni l'assuré.

1. Blockchain : Scénario ?



1. Blockchain : Cas d'applications qui existent …. déjà !

Guardtime: 2007
Projet de la start-up avec le gouvernement estonien pour sécuriser les 1 million de dossiers médicaux sur la blockchain.
Les actifs seraient les dossiers numérisés des patients

guardtime

Bitcoin : 2009
système monétaire numérique et cryptographique inventé par Satoshi Nakamoto, disponible en open-source.
L'actif serait la transaction monétaire (métadonnée)

Etherum: 2013
Un protocole d'échanges décentralisés permettant l'accomplissement de contrats intelligents. Du terme Ether qui est l'unité de paiement de ces contrats.
l'actif serait l'ensemble des termes du contrat

1. Blockchain : Objectif ?

Convergence vers un monde où **la seule autorité de confiance** serait : **LES PROGRAMMES**
Déléguer aux systèmes Blockchain :

- la confiance
- l'automatisation
- la sécurité

1. Blockchain : Potentiel applicatif

Domaine monétaire

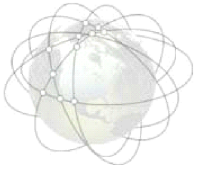
- Transactions inter-bancaires
- Titre bancaires
- Actions

Domaine contractuel

- Tout type de contrat (exécution automatique des termes)

Domaine de la santé

- Certification des médicaments dans le monde, pour combattre les médicaments contrefaits et dangereux.
- Certification et protection des dossiers patients avec approbation par tous les professionn de santé impliqués.



Merci …