DRAFT

COMPRENDRE LA BLOCKCHAIN

Comprendre et anticiper le potentiel de disruption de la Blockchain

Ce document constitue un DRAFT
et est amené à évoluer

Réalisé par Amine HAMOUDA

Niji

1. Contexte & genèse de la Blockchain
2. La Blockchain
3. Concepts de
4. Glossaire de Blockchain
5. Annexes et Sources

CONTEXTE

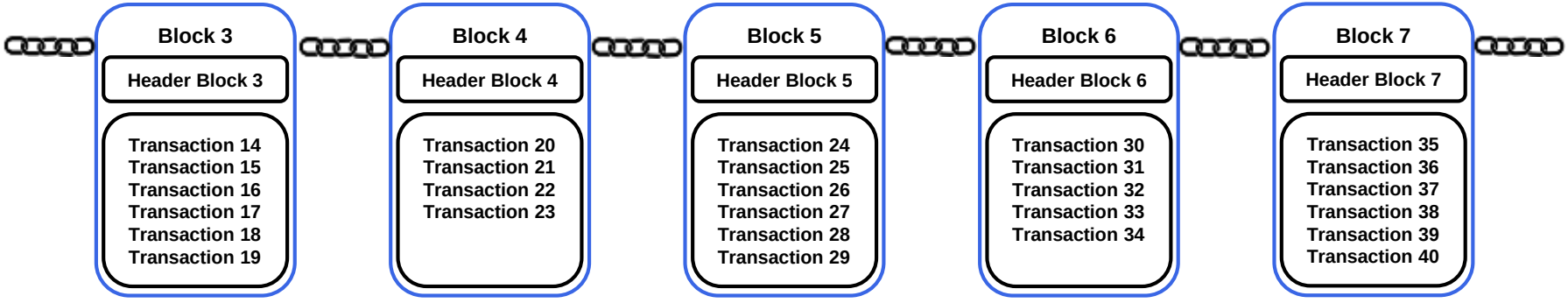
1 – ÉLÉMENTS DE CONTEXTE

- Dans un contexte de **crise économique** (2008-2009), de **scandales financiers et monétaires**, de **perte de confiance** en les institutions bancaires, un groupe de *hackers* a crée une **crypto-monnaie** émise par un système d'échange entre pairs et dénué de tout système de contrôle centralisé. C'est ainsi que **Satoshi Nakamato** pose les principes fondateurs de **Bitcoin** dans en 2009 (lien)
- Blockchain est **l'architecture et le paradigme** sous-jacent au Bitcoin**.**
  - Bitcoin est le *use-case* monétaire de Blockchain (et accessoirement le *use-case* le plus connu)
- Blockchain est souvent victime de préjugés négatifs et de l'amalgame avec Bitcoin
  - Origine nébuleuse de Bitcoin
    - Satoshi Nakamato (Craig Wright de son vrai nom) est-il une personne physique? Est-ce un groupe de hackers? Pour qui agissent-ils? Qui maitrise les nœuds du réseaux?...)
  - Quelques scandales : Achats illégaux, blanchiment d'argent et vols
    - En 2014, vol de l'équivalent de 400 M$ en bitcoin à Mt.Gox
    - En 2015, BitPay
    - Découverte régulière de malwares


BLOCKCHAIN

QUÈSACO

- La Blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle
- La Blockchain constitue une base de données (*Ledger* ou registre) qui contient l'historique de tous* les échanges (transactions) effectués entre les utilisateurs depuis sa création. Cette base de données est sécurisée (chiffrage), distribuée (à tout les utilisateurs) et sans intermédiaire

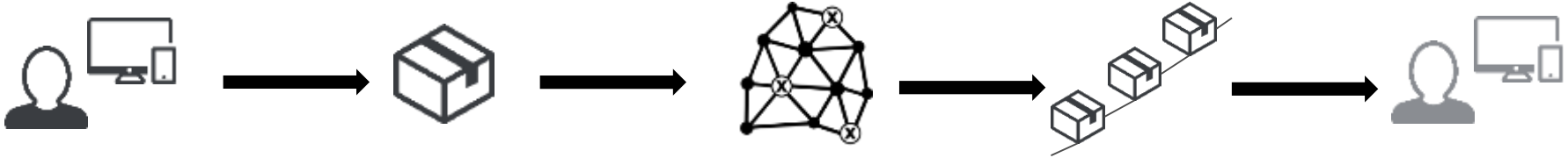


- Blockchain peut est assimilée à un grand livre comptable public, anonyme et infalsifiable.

(*) *Tous les échanges en théorie car avec l'explosion du nombre de transactions, des systèmes de type clients légers, notamment destinés au applications mobile, est en train de voir le jour*

COMMENT CA MARCHE?

- Toute Blockchain publique fonctionne nécessairement avec une monnaie ou un token (jeton) programmable
- Les transactions effectuées entre les pairs (aussi appelé nœuds du réseau) sont regroupées par blocs.
- Chaque bloc est validé par les nœuds du réseaux via un mécanisme de consensus (voir slide mécanismes de consensus). Dans le cas de la blockchain de bitcoin, cette technique est appelée le « Proof of Work » (ou minage) (voir partie concepts pour plus de détail)
  - Concrètement, le premier nœud qui *mine* le bloc s'attribue la Proof-of-Work et, est donc rétribué. Des mécanismes de consensus permettent de gérer les doubles minages et d'arriver à un consensus rapidement (mise en compétition des *miners* qui augmente la puissance de calcul du réseau)
- Un fois validé, le bloc est horodaté et ajouté à la chaine de bloc et partagé à l'ensemble des nœuds du réseau. La transaction est alors visible de tout le réseau.



Un utilisateur A effectue une transaction vers B

Les transactions sont **regroupées** dans un **bloc**

Le bloc est **validé** par les nœuds du réseau via des **mécanismes de consensus**

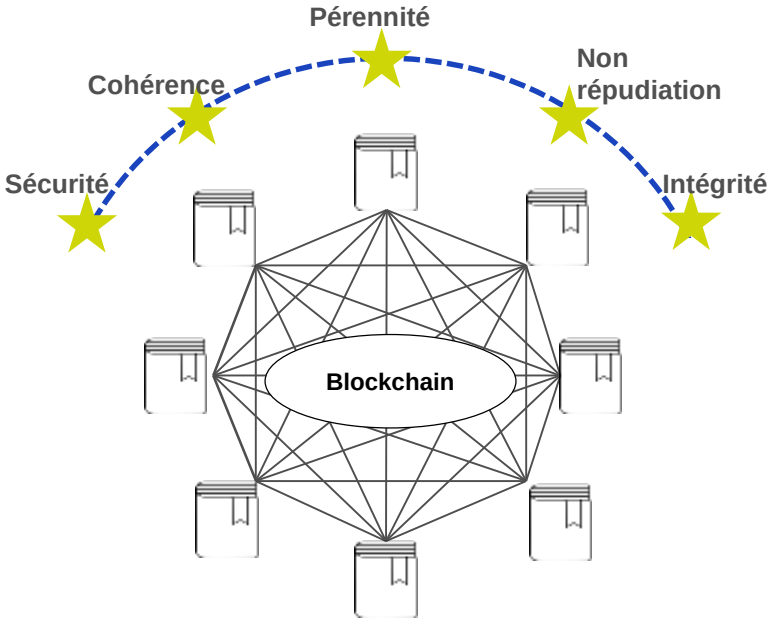
Le **bloc miné** est alors daté et ajouté à la chaine de blocs

L'utilisateur B reçoit la transaction

AVANTAGES ET LIMITES DE LA BLOCKCHAIN

Les avantages

- Sécurité, décentralisation et dématérialisation des transactions et des *assets*
- Réduction des couts à travers
  1. La suppression du thiers de confiance
  2. Automatisation et simplification
- Dématérialisation d'un certain nombre de processus
- Atténuation des risques (risque répartie sur l'ensemble des nœuds du système et plus sur un thiers de confiance)



Limites

- Problématique juridique
- Vitesse d'exécution des transactions
- Passage à l'échelle pour de grands volumes de transaction
- Evolution du protocole
- Cout d'implémentation actuel
- Sécurité (au sens écosystème)

CONCEPTS

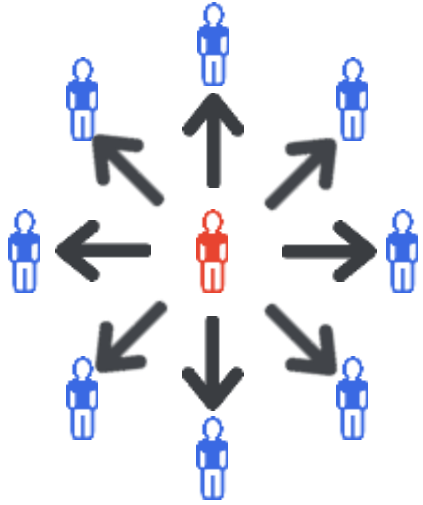
MODÈLE CENTRALISÉ ET RÔLE DU TIERS DE CONFIANCE

Principe :

Dans un modèle centralisé, un tiers de confiance (*middle men*) joue le rôle d'intermédiaire dans les échanges entre les différents intervenants du system

Quel rôle joue le tiers de confiance?

- Il facilite les échanges entre les intervenants
- Il est le garant de la sécurité et de l'intégrité des échanges



Quelques exemples de systèmes centralisés :

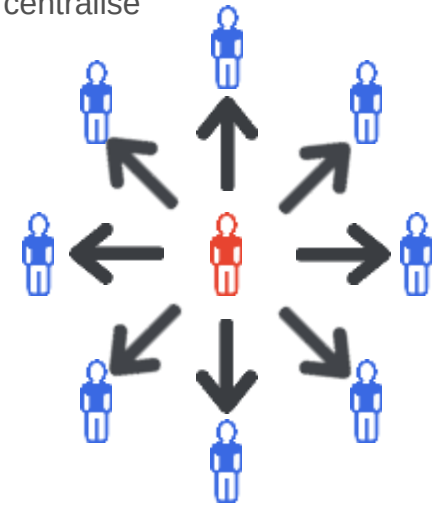
- Le système bancaire
- Le système notariale
- Le système de vote
- Une base de données standard
- *Guiness Book* des records

Les limites de ce système :

- Forte dépendance au tiers de confiance
- Le tiers de confiance constitue un point de défaillance potentiel (anti-pattern : *single point of failure*)
- Nécessite la confiance en le tiers de confiance
- Ajout de processus supplémentaires et donc d'un surcout économique
- Limitant en terme de passage à l'échelle

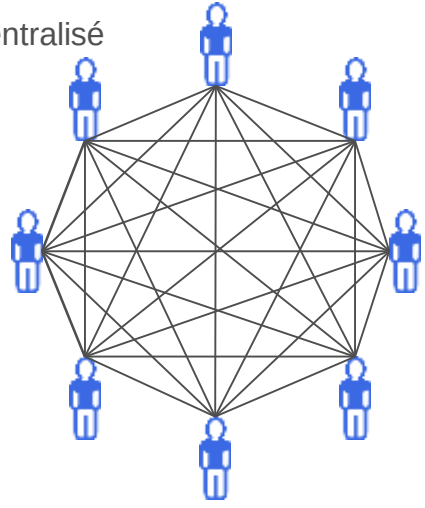
MODÈLE CENTRALISÉ VS. DÉCENTRALISÉ

Modèle centralisé



- Pas de confiance requise entre les pairs
- Contrôle de l'information et des échanges
- Point de défaillance
- Confiance en le tiers requise
- Pairs dépendant du tiers de confiance

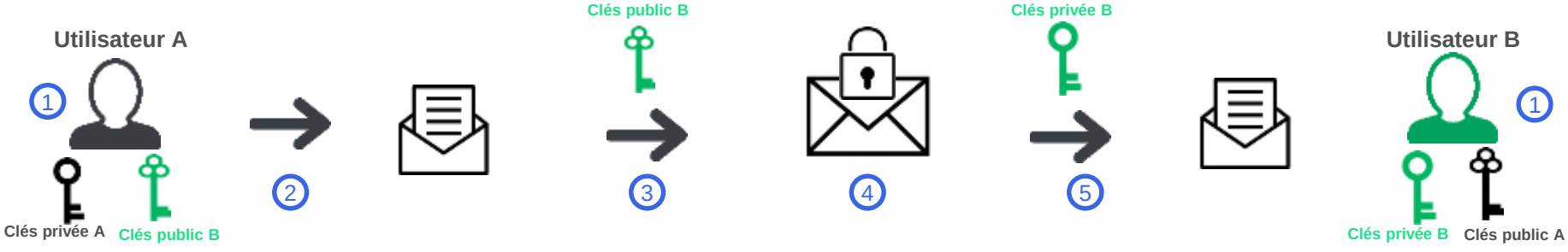
Modèle décentralisé



- Pas de confiance requise entre les pairs
- Pas de point de défaillance
- Pas de dépendance à un tiers de confiance ou à un pair
- Processus supplémentaires requis pour créer le consensus, assurer la sécurité et la transmission de l'information)
- Difficulté d'accès à l'information
- Difficulté à faire évoluer le protocole

CLÉS PUBLIQUE / CLÉS PRIVÉE

- L'utilisation d'une paire **clés publique/clés privée** est un des principe sur lequel repose la **cryptographie asymétrique** (une méthode de chiffrement).
- Principes :
  1. Chaque utilisateur dispose d'une **clés publique** qu'il **diffuse** et d'une **clé privée** qu'il **garde**
  2. Un utilisateur A souhaite envoyer un message m à un utilisateur B
  3. L'utilisateur A chiffre le message m avec la clés publique de l'utilisateur B
  4. L'utilisateur B reçoit le message m chiffré avec sa clés publique B.
  5. L'utilisateur B est le seul à pouvoir déchiffrer le message m chiffré avec sa clé privée B



MÉCANISMES DE CONSENSUS

Les mécanismes de consensus sont utilisés pour s'assurer que tout les nœuds du réseau (paires) disposent des mêmes informations et que seules les transactions valides sont enregistrées dans les registres distribués. En d'autres termes, il s'agit de la manière de valider les blocs de la Blockchain

- **Proof of Work** (Preuve de travail ou PoW) constitue le processus de résoudre un défi informatique imposé par une Proof of Work est appelé **mining** (on parle de **mineurs).** Les mineurs doivent résoudre un problème informatique ayant une difficulté d (d est variable et évolue en fonction de la puissance de calcul du système) pour valider un block. La Proof of Work est utilisé par la Blockchain de Bitcoin

- **Proof of Stake** (Preuve d'enjeu ou de possession ou PoS) constitue le processus de résoudre un défi informatique imposé par une Proof of Stake est appelé **minting** (on parle de **forgeurs)**. La Proof of Stake se base sur la probabilité qu'un nœud parvienne le prochain block de transactions à ajouter à la Blockchain est proportionnelle à la quantité de monnaie que possède ce nœud. Les forgeurs doivent résoudre un problème informatique pour valider un block.

- Il existe d'autres mécanismes de consensus comme le **Practical Byzantine Fault Tolerance (PBFT)** basé sur le problème des généraux byzantins (métaphore informatique) et le **Zero Knowledge Proof** (un *fournisseur de preuve* prouve mathématiquement à un *vérificateur* qu'une proposition est vraie sans toutefois révéler d'autres informations que la véracité de la proposition)

NB : Voir annexe pour le détail des problèmes informatiques PoS et PoW

LE CONCEPT DE TOKENISATION

- Les *ledgers* (registres) de la plupart des blockchains reposent sur des assets digitaux appelés Tokens (jetons)
  - Dans la blockchain **Ripple**, les tokens sont nommés **XRP**
  - Dans la blockchain d'**Ethereum**, les tokens sont nommés **Ethers**
- Les Tokens servent deux objectifs principaux
  - Rémunérer les nœuds du réseaux lors du processus de minage et donc encourager la définition d'un consensus
  - Prévenir des SPAM et attaques de types *Deni de Services*

GLOSSAIRE

LEXIQUE DE LA BLOCKCHAIN

A compléter

Altcoin : Abréviation de l'expression « Alternative Coin ». Une altcoin est une cryptomonnaie autre que le bitcoin (e.g Citicoin, ether, amazoncoin…)

Bitcoin (BTC) : Cryptomonnaie électronique décentralisée conçue en 2009 par Satoshi Nakamato

Blockchain : ou « Chaine de block » est un paradigme de stockage décentralisé et de transmission d'informations à cout réduit, sécurisé et transparent. Blockchain peut être assimilée à une base de données sécurisée et distribuée et à un grand livre comptable public, anonyme et théoriquement infalsifiable

Fonction de Hachage : On nomme fonction de hachage une fonction particulière qui, à partir d'une donnée fournie en entrée, calcule une empreinte servant à identifier rapidement, bien qu'incomplètement, la donnée initiale. Les fonctions de hachage sont utilisées en informatique et en cryptographie

Hash : Résultat que produit une fonction de Hachage

Ledger : Registre dans lequel sont enregistré les transactions d'un systeme

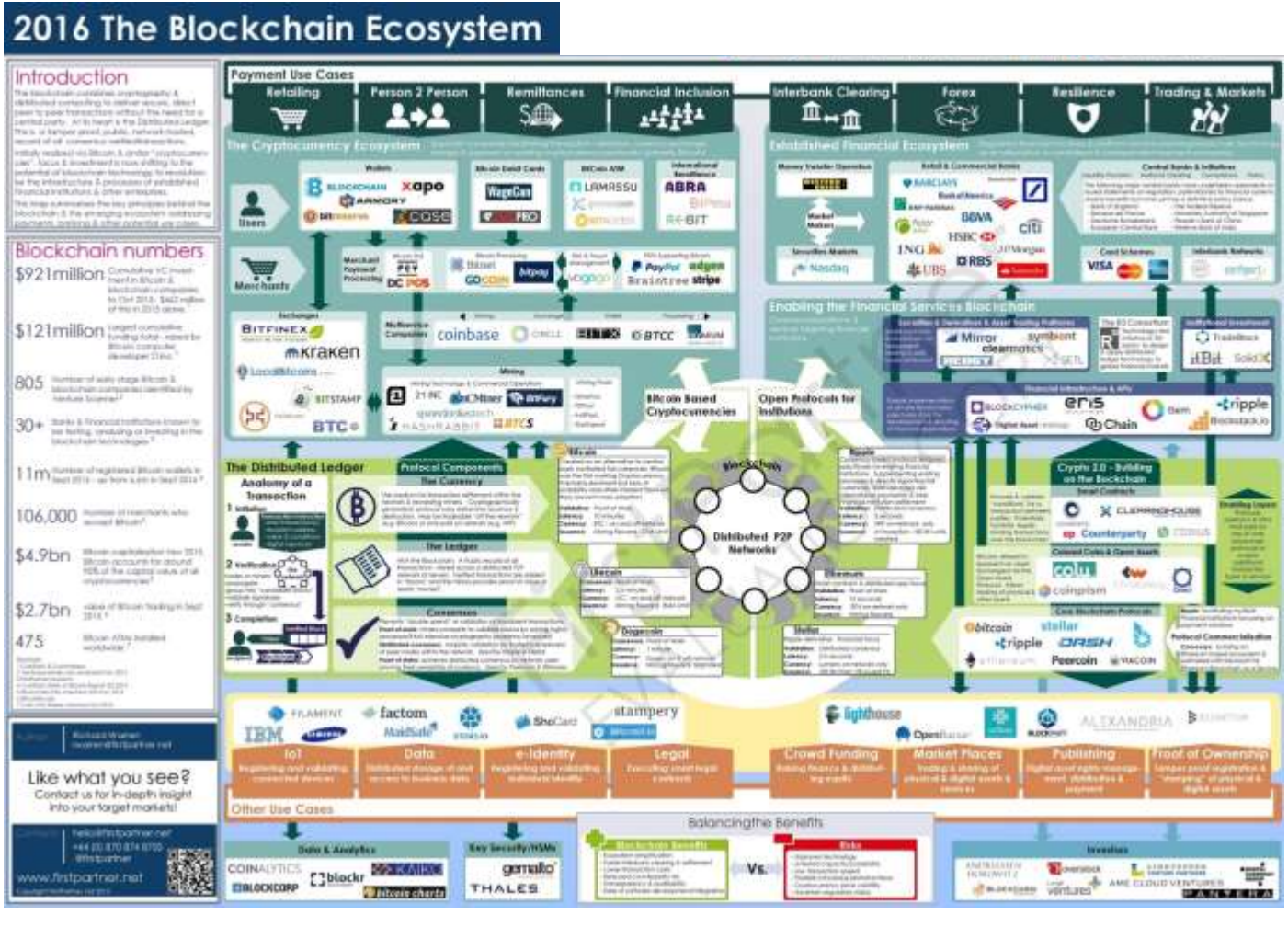
Minage : utilisation de la puissance de calcul informatique afin de traiter des transactions, sécuriser le réseau et permettre à tous les utilisateurs du système de rester synchronisés

Noeud : ordinateur relié au réseau et utilisantun programme relayant les transactions

UTXO : Etat du système à un instant t ou encore un » collection d'outputs de transactions non dépensées

ANNEXES & SOURCES

ECOSYSTÈME BLOCKCHAIN



Source : FirstPartner

POS VS. POW

- Proof of Work
  - Pour faire référence à un bloc spécifique de la blockchain, on fait le hash (SHA-256) de son header deux fois. L'entier résultant appartient à l'intervalle [0, 2^256 – 1]
  - Dans la PoW, pour qu'un bloc soit considérée valable, cet entier ne doit pas excéder le seuil : **hash(B) ≤ M/D** D représentant la difficulté de la tache D ∈ [1,M]
  - Il n'y a aucune façon connue de prédire à l'avance quel argument B va satisfaire cette équation
- Proof of Stake
  - Prenons un utilisateur A avec un solde bal(A). Une fonction de PoS utilisera cette condition
  - **hash(hash(Bprev), A, t) ≤ bal(A) M / D**
  - **Bprev** représente le bloc sur lequel l'utilisateur est en train de construire
  - T est le timestamp

SOURCES

Livres :

- Blockchain, Blueprint for new economy, Melanie SWAN – O'Reilly

Blogs et sites web :

- Principes fondateurs de Bitcoin de Satoshi Nakamoto - https://bitcoin.org/bitcoin.pdf
- Blogchaincafe - http://blogchaincafe.com/ - David TERRUZI
- Finyear - http://www.finyear.com/
- Blockchain France - https://blockchainfrance.net/
- Practical Byzantine Fault Tolerance (PBFT) - http://pmg.csail.mit.edu/papers/osdi99.pdf

Whitepapers :

- Bitcoin : A Peer-to-Peer Electronic Cash System
- Comprendre la Blockchain – édite par U – plateforme de transformation digitale

MERCI DE VOTRE ATTENTION

AMINE.HAMOUDA@NIJI.FR
06.25.25.31.65

@AMINE_HAMOUDA86

LIEN