MOHAMMED VI POLYTECHNIC UNIVERSITY

Blockchain, une décennie d'évolution

Journée ASMEX
Blockchain menaces ou opportunités sur le commerce extérieur national

MSDA
MODELING SIMULATION & DATA ANALYSIS

Agenda

- Une brève histoire de la blockchain
- Qu'est ce que la technologie blockchain
- Les piliers et les offres de la blockchain
- Gouvernance d'une blockchain
- Quand la blockchain fait sens ?
- Quelques exemples de blockchain et ecosystème.

Une brève Histoire de la Blockchain1/2

- Au commencement était la monnaie. De la monnaie primitive à fiduciaire et scripturale. Cet instrument de transaction repose sur la confiance, celle que lui accordent les utilisateurs. Cette confiance s'appuie sur un principe de garantie incarné par une **institution centralisée**. (Etats, Banques, …)

- La dématérialisation de la monnaie, du chèque à la carte de paiement et au transactions éléctroniques a ouvert la voie à une réflexion sur la création de monnaie non conventionnelle: Indépendantes des autorités centralisées traditionnelles, ce sont les **monnaies digitales**.

- La monnaie digitale diffère de la monnaie traditionnelle, pièces, billets ou de leur version dématérialisée car elle repose sur un **protocole de chiffrement ou cryptographique**. Chaque unité de monnaie digitale est une **chaîne de nombres unique** que les utilisateurs peuvent s'envoyer en ligne lors des transactions.

Une brève Histoire de la Blockchain 2/2

- Echec des premières tentatives confrontées à un défi de taille: **La sécurité**.

- En 1990, David Lee Chaum, Cryptographe, Mathématicien et concepteur de la monnaie éléctronique "*DigiCash*" apporte une solution en créant un registre central de toutes les transactions.

- En octobre 2008, Satoshi Nakamoto, don't l'identité de la personne ou du groupe caché derrière ce pseudonyme reste à ce jour inconnue, publie un livre blanc "*Bitcoin: A Peer-to-Peer Electronic Cash System*" où il propose une nouvelle forme de monnaie digitale, le "Bitcoin" qui se fonde sur un protocole nouveau, celui d'une chaîne de blocs ou "**Blockchain**" permettant un système de vérification décentralisé mais sur une relation dite "pair-à-pair".

- La blockchain de Bitcoin a été lancée le 3 Janvier 2009 à 18h15 UTC et compte aujourd'hui près de 400000 blocs.

Qu'est ce que la technologie Blockchain

- La **blockchain** est juste **une écriture comptable d'opérations numériques, partagées entre de multiples acteurs.** Autrement dit**: Un registre digitale où chaque page et un bloc.**

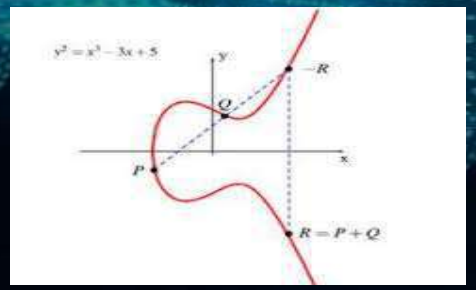
- Elle ne peut être **mise à jour que par consensus entre une majorité de participants** au système. Et, une fois entrée, l'information ne peut **jamais être écrasée**.

- La blockchain est une base de données distribuée entre des **acteurs ne se faisant pas confiance.**

Les piliers et les offres de la Blockchain

Blockchain

Mathématique :
La Cryptographie Asymétrique
ECC Elliptic Curve Cryptography



Technologique :
Système Distribué proche du modèle client-serveur mais où chaque client est aussi serveur
Où chaque acteur du réseau à le même statut.
Chaque acteur possède une copie de l'état actuel des transactions

Sociologique :
Modèle transactionnel dont l'architecture est en mode « pair-à-pair » nécessitant un consensus distribué sans un tiers de confiance

- Le stockage et la transmission de l'information : une BDD / livre de compte/registre.
- Entre personnes individualisées : des méthodes d'identification sécurisées et chiffrées.
- Sans intermédiaire défini : distribué entre ses participants.
- Transparente: publique et librement accessible, au moins pas ses utilisateurs.
- Sécurisée : avec un protocole de consensus resistant aux attaques.

Quelle gouvernance pour la Blockchain ?

- La transmission des transactions entre acteurs de manière cryptée, ECC.
- Des transactions possédant une empreinte numérique unique (Hashage).
- Des transactions inaltérables et durables dans le temps : il est possible de prouver l'existence et la non modification d'une transaction passée.
- Consensus distribué : c'est un protocole dont le choix n'est pas anodin.
  - Il garantit que le bloc N+1 dans la chaine est le seul et unique version qui contient le vérité des transactions.
  - Protège la chaine contre des attaques.

Blockchain publique sans authentification des acteurs

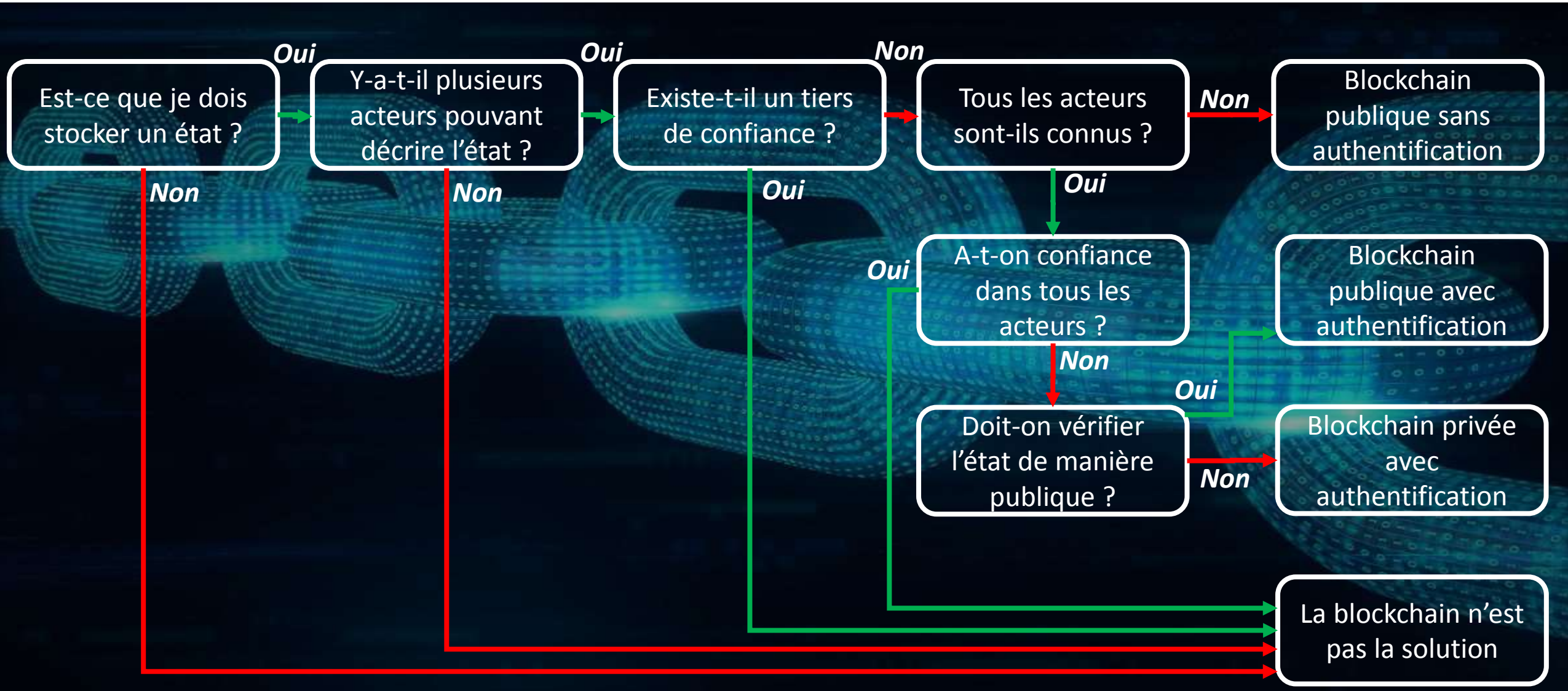
Blockchain hybride / privée avec authentification des acteurs

Choix du protocole de consensus en fonction du type de blockchain

Protocoles de consensus:

- Proof of Work.
- Practical Byzantin Fault Tolerance
- Proof of Elapsed time
- Proof of Activity
- Proof of Capacity
- Et autres

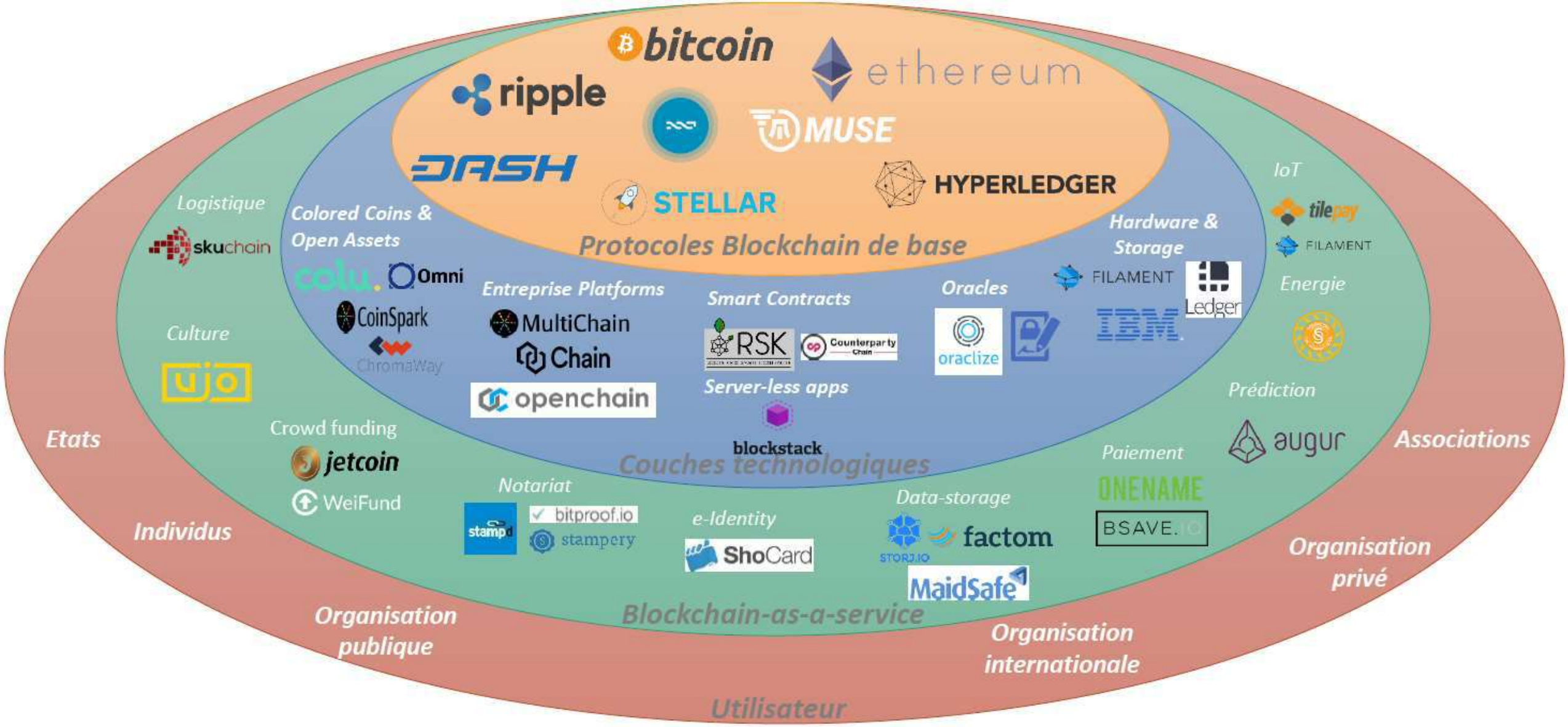
Dans quelle situation la blockchain fait sens ?



Les principales Blockchain

	Bitcoin	Ethereum	Hyperledger Fabric
Recours à une cryptomonnaie	***Bitcoin***	***Ether***	***Non***
Accès au réseau	***Sans permission***	***Sans ou avec permission***	***Avec permission***
Transactions	***Anonyme***	***Anonyme ou privé***	***Public ou confidentiel***
Consensus	***Proof Of Work***	***Proof Of Work***	***PBFT***
Logique de smart contracts	***Non***	***Oui (Solidity, Serpent, LLI)***	***Oui (Chaincode)***
Langage	***C++***	***Golang, C++, Python***	***Golang, Java***

Ecosystème autour de la Blockchain



Contact

Hassan BALOUI

Université Mohammed VI Polytechnique

Modeling Simulation & Data Analysis

hassan.baloui@um6p.ma