

ATELIER BLOCKCHAIN & CYBERSÉCURITÉ
AGENCE NATIONALE DE LA SECURITE INFORMATIQUE, 06 FÉVRIER 2020

Blockchain et Cryptomonnaies : Concepts de base et applications

HANEN IDOUDI

MAÎTRE DE CONFÉRENCES EN INFORMATIQUE, HDR
ECOLE NATIONALE DES SCIENCES DE L'INFORMATIQUE
UNIVERSITÉ DE LA MANOUBA
HANEN.IDOUDI@ENSI-UMA.TN



جامعة منوبة
Université de la Manouba

Plan

- ▶ La naissance de la technologie Blockchain
- ▶ Les cryptomonnaies
- ▶ Blockchain : fonctionnement général
- ▶ Les types de Blockchain (privée, publique)
- ▶ Les applications de la Blockchain
- ▶ Quelques plateformes Blockchain

Le commencement ...

- ▶ Contexte mondial : Récession de 2007-2012
- ▶ 2008 : Crise financière
 - ▶ Faillite de 11 banques dont la banque d'investissement Lehman Brothers

Climat de manque de confiance en les institutions bancaires

- ▶ **Naissance de BITCOIN par Satoshi Nakamoto**
 - ▶ Annoncé en 2008, premier bitcoin créé en 2009
 - ▶ **Crypto-monnaie** émise par un système d'échange entre pairs et dénué de tout système de contrôle centralisé



Le commencement ...

« **Bitcoin** est une technologie pair à pair fonctionnant sans autorité centrale. La gestion des transactions et la création de bitcoins est prise en charge collectivement par le réseau. **Bitcoin est libre et ouvert. Sa conception est publique, personne ne possède ni ne contrôle Bitcoin et tous peuvent s'y joindre.** » - www.bitcoin.org

Bitcoin : monnaie virtuelle + protocole



Les monnaies virtuelles, cryptomonnaies

*"Une représentation numérique de la valeur qui n'est ni émise par une banque centrale ou une autorité publique, ni nécessairement rattachée à une monnaie officielle, mais qui est acceptée par les personnes physiques ou morales comme moyen de paiement et qui peut être transférée, stockée ou négociée électroniquement". - **Autorité bancaire européenne, 2014.***

- ▶ Fin 2019 *
- ▶ Prés de 2 400 cryptomonnaies
- ▶ Market Capitalization : \$196 291 264 042 • BTC Dominance: 66.5%

* Source : <http://coinmarketcap.com>

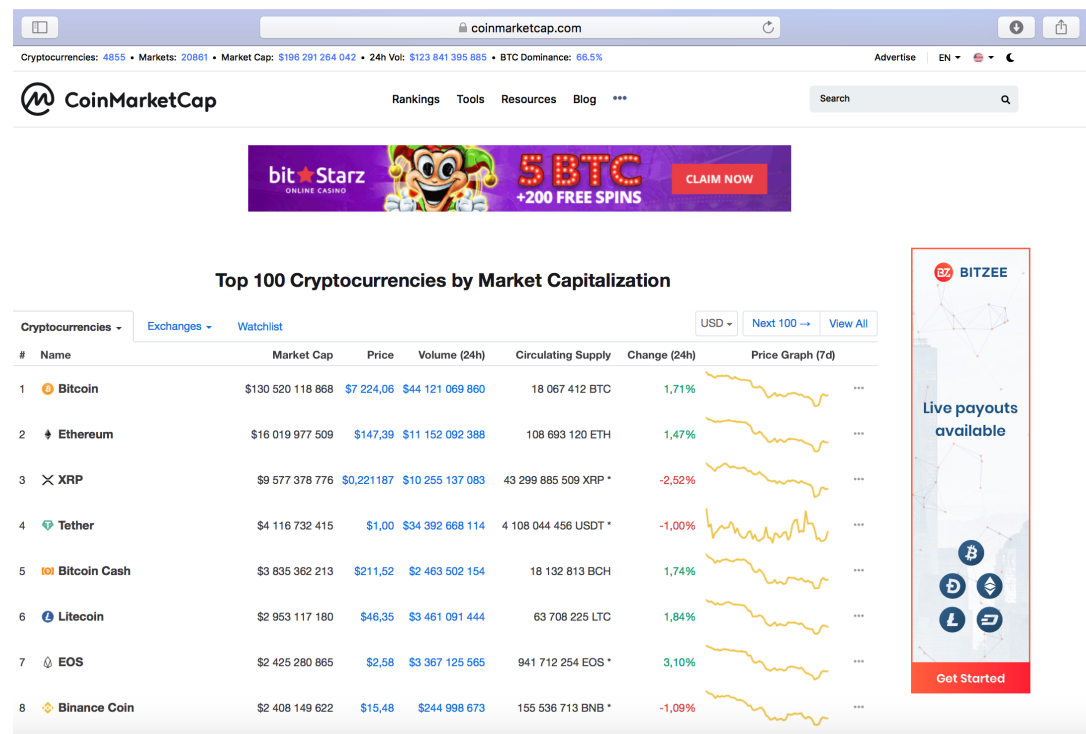
Les monnaies virtuelles, cryptomonnaies

Code	Monnaie	Création
BTC, XBT	Bitcoin	2009
ETH	Ethereum	2015
BCH, BCC	Bitcoin Cash	2017
XRP	Ripple	2012
LTC	Litecoin	2011
EOS	EOS	2017
Thether	Thether	2015
XTZ	TEZOS	2018



libra

- ▶ Projet initié par Facebook et projetée pour 2020
- ▶ Fondation de 28 entreprises à son lancement en 2019

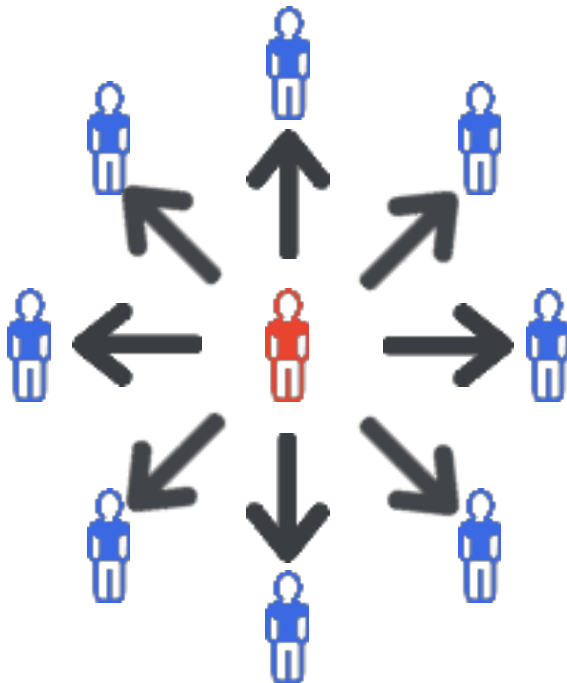


... Et la BLOCKCHAIN dans tout ça ??

- ▶ **Blockchain est l'architecture et le paradigme sous-jacent au Bitcoin**
- ▶ Technologie **reprise, améliorée et adaptée par d'autres plateformes** plus tard.
- ▶ Technologie de stockage et de transmission d'informations, **transparente, sécurisée**, et fonctionnant **sans organe central de contrôle**
- ▶ Utilise une base de données (**Ledger ou registre**) qui contient l'historique de tous les échanges (**transactions**) effectués entre les utilisateurs depuis sa création.
- ▶ L'échange de crypto-monnaie est le premier use case de cette technologie

La BLOCKCHAIN, QUESACO ?

Modèle centralisé : Tiers de confiance



Exemples

- Systèmes bancaires
- Systèmes de votes
- Vente en ligne (modèle de paiement classique)

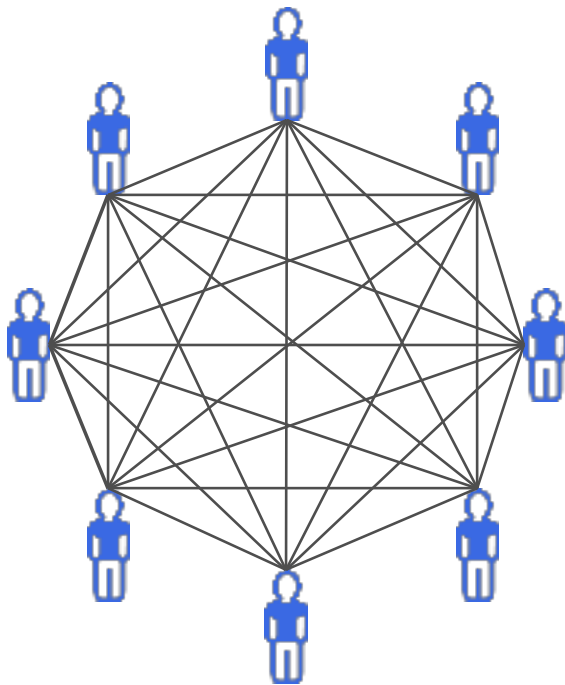
Limites

- **A-t-on confiance au tiers de confiance ??**
- **Single point of failure**
- **Limitant en terme de passage à l'échelle**
- **Coût économique supplémentaire**

La BLOCKCHAIN, QUESACO ?

9

Modèle décentralisé ou pair à pair



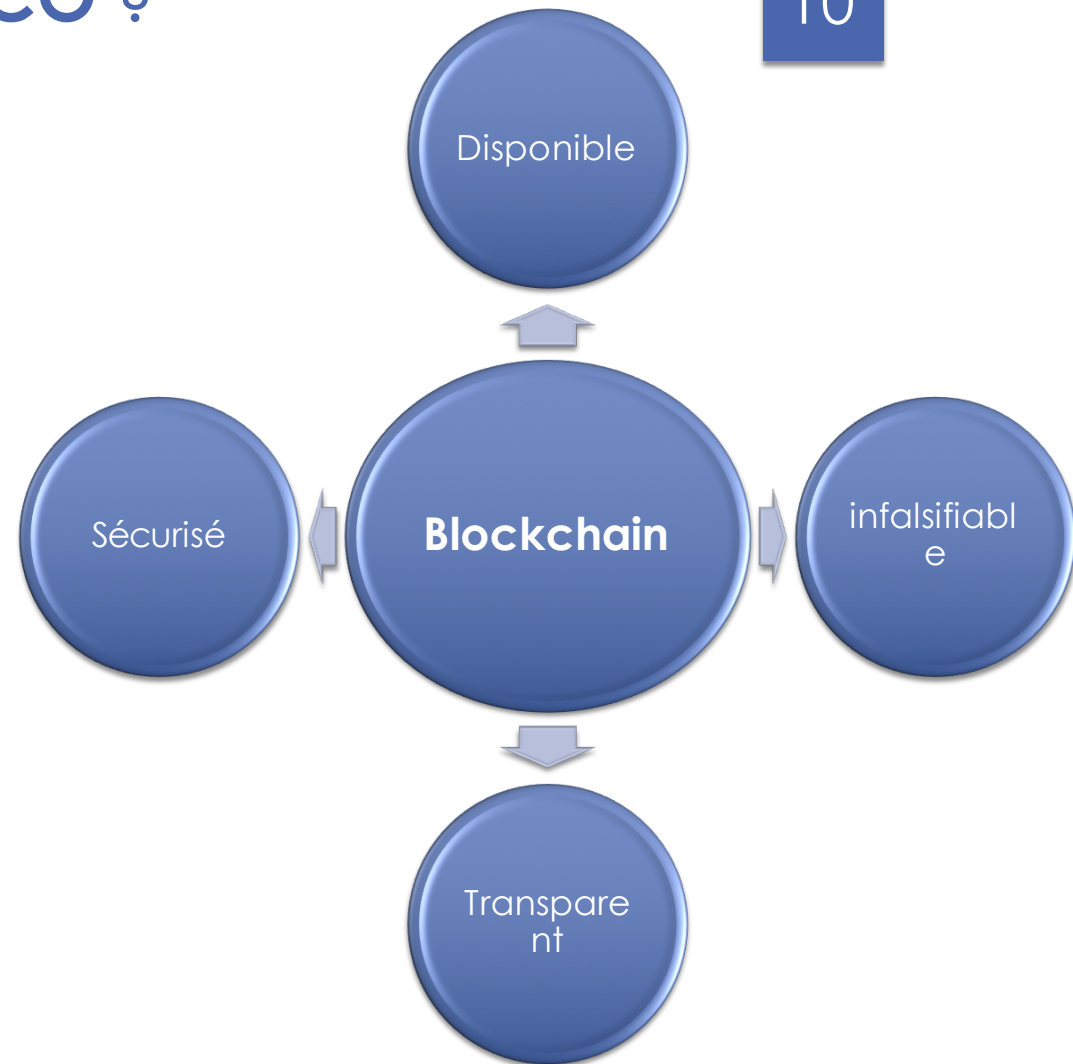
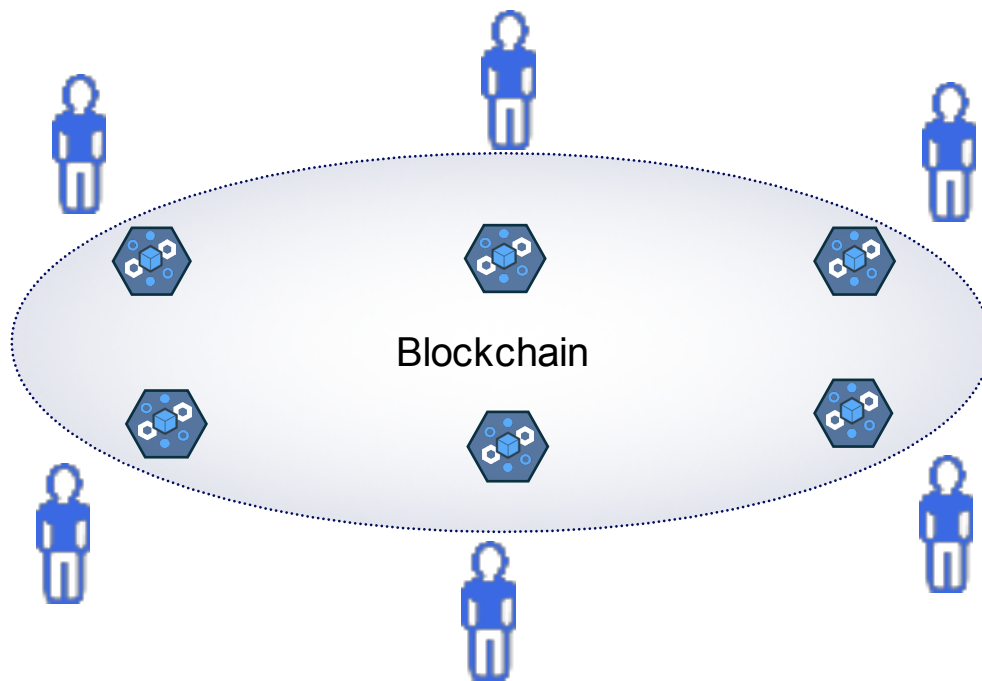
Avantages

- Pas de dépendance à un tiers de confiance
- Pas de point de défaillance

La BLOCKCHAIN, QUESACO ?

10

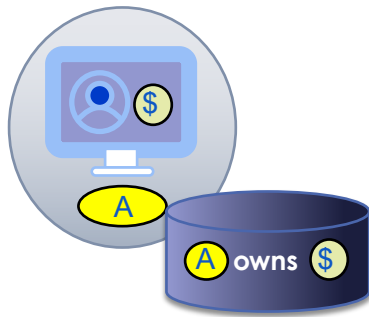
Registre (**Ledger**) de données répliqué entre tous les intervenants



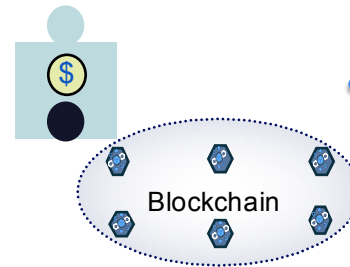
La BLOCKCHAIN, QUESACO ?

11

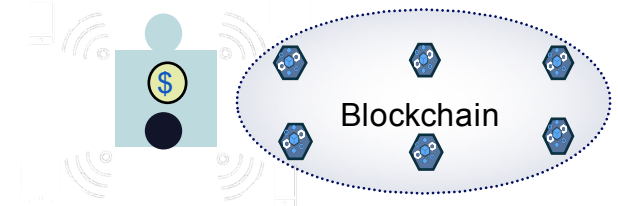
1 A veut transférer un asset à B



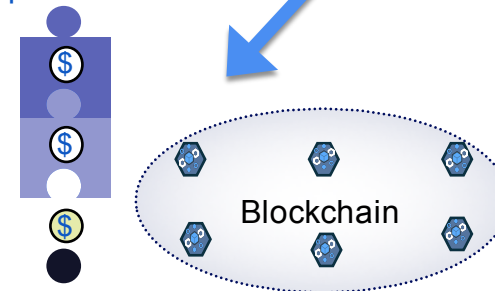
2 Un ensemble de **transactions** est regroupé dans un block puis diffusé



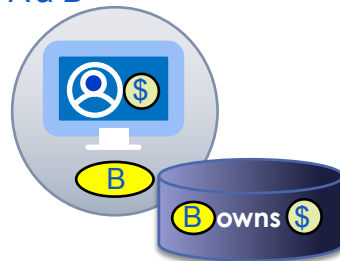
3 Le block est validé par tous les participants par un mécanisme de **Consensus**



4 Le block est ajouté à la chaîne par tous les participants



5 L'asset est transféré de A à B



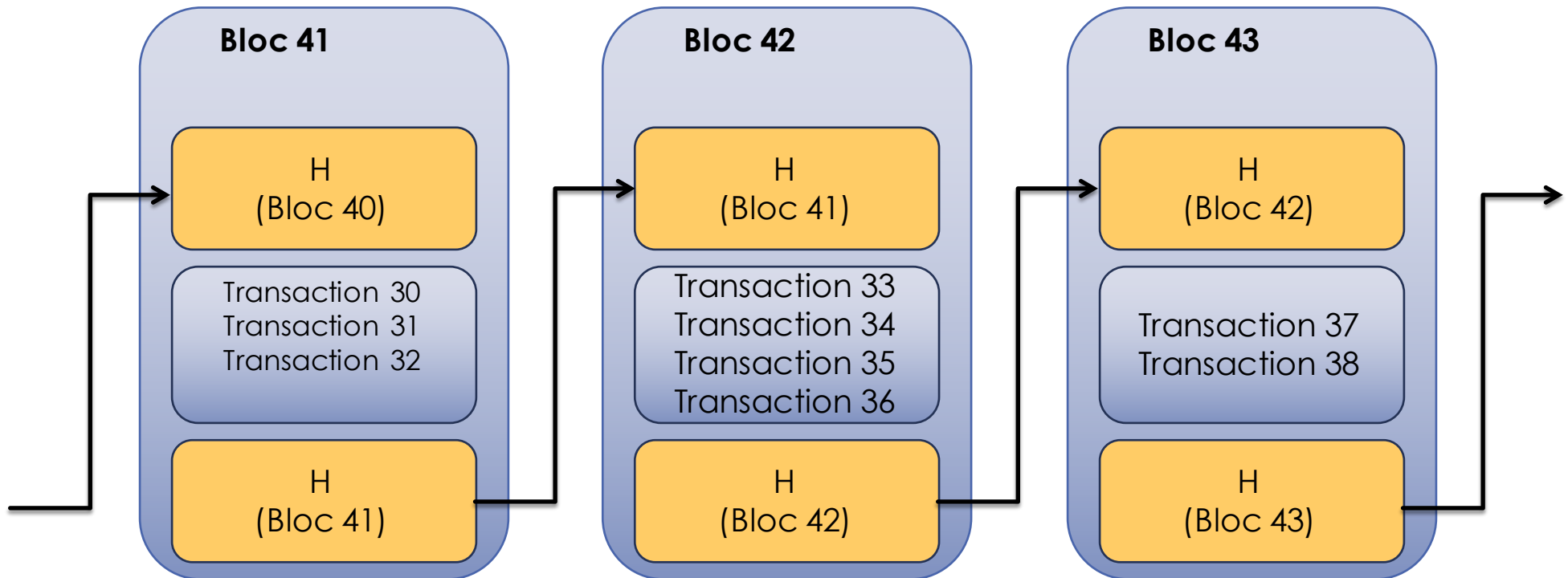
La BLOCKCHAIN, QUESACO ?

12

Chaine de blocs



Append Only !!!

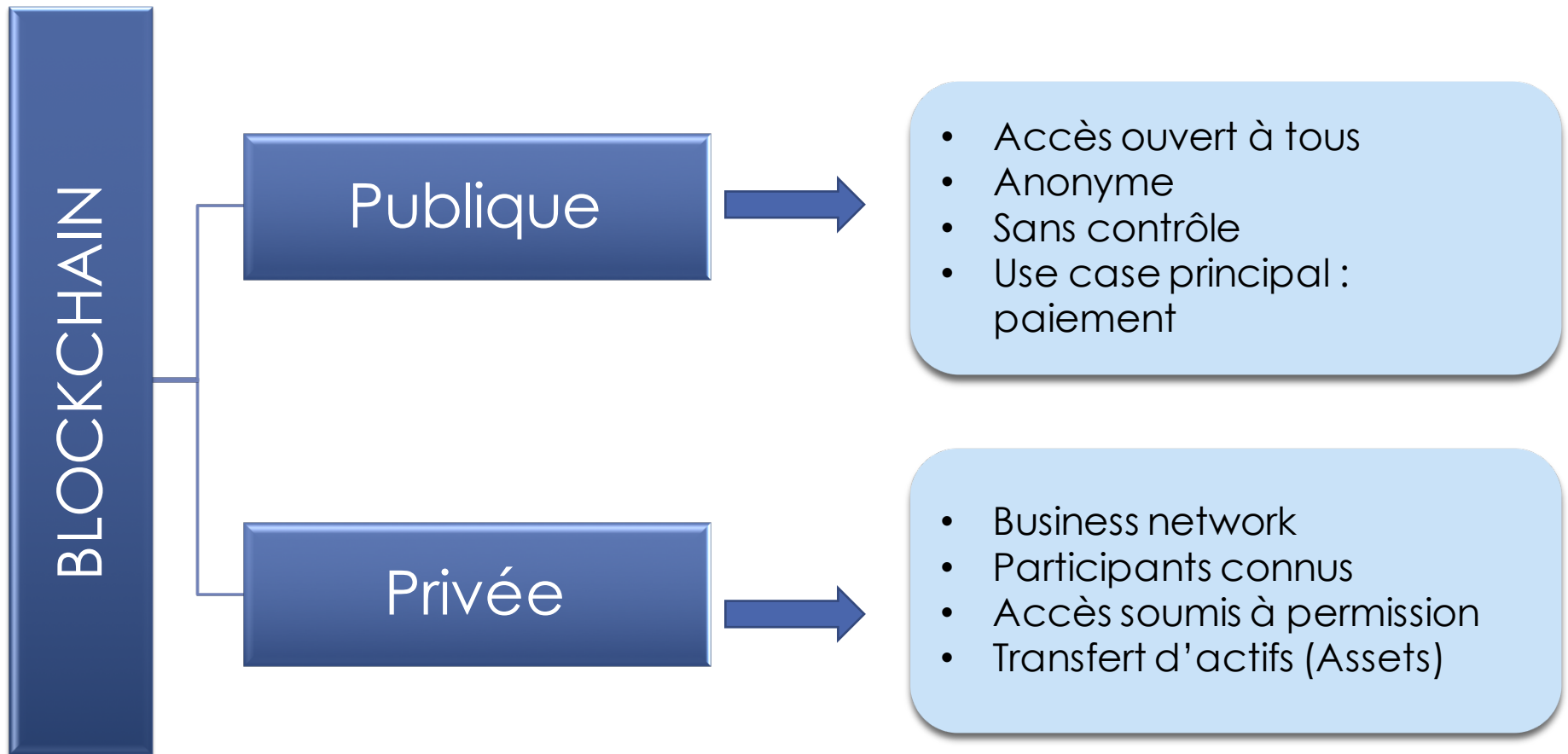


Les contrats intelligents

- ▶ Introduits en 2011
- ▶ Implémenté par Ethereum (2015) pour la 1ère fois
- ▶ Permet de définir comment un système à base de Blockchain peut fonctionner
 - ▶ Comment les transactions sont validées, exécutées

Les Smart Contracts sont des scripts, ou des codes, écrits et déployés dans la blockchain, dans l'attente que certaines conditions soient vraies ou fausses, afin de déclencher une action ou une transaction spécifique.

Les types de BLOCKCHAIN



Les types de BLOCKCHAIN - Publique

- ▶ Sans permission
- ▶ Anonyme
- ▶ Transparente

- ▶ Quiconque peut rejoindre le réseau
 - Participer au processus de vérification des bloc (consensus)
 - Créer des contrats intelligents
 - Générer des transactions

- ▶ **BITCOIN !**

Les types de BLOCKCHAIN - Privée

- ▶ Accès par autorisation
- ▶ Identité des participants connue et vérifiée
- ▶ Le principe de consensus est vérifié par un nombre limité et prédéfini de participants.
- ▶ **Blockchain de consortium**
 - ▶ Regroupe plusieurs acteurs qui possèdent des droits.
 - ▶ Les décisions sont prises par la majorité des acteurs.

BLOCKCHAIN FOR BUSINESS

Blockchain privée

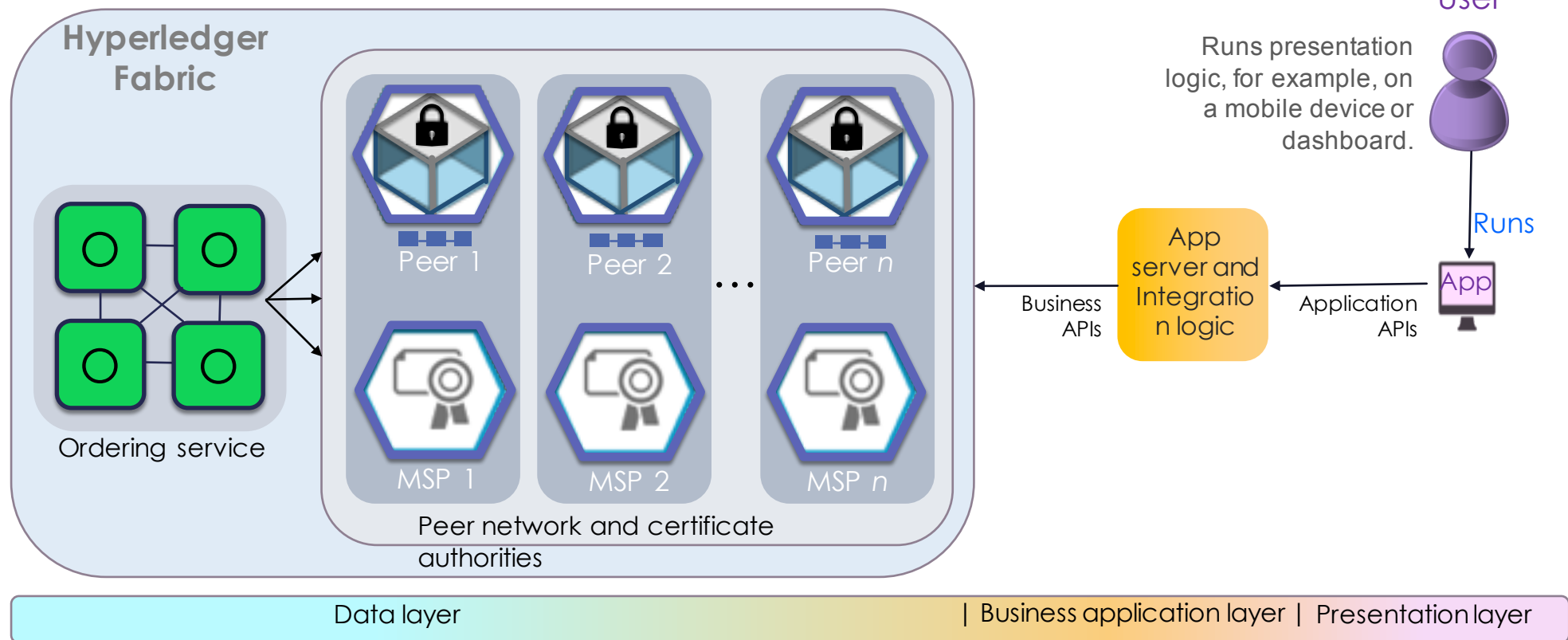
- *Identités connues*
- *Nœuds validateurs sélectionnés*
- *Transfert d'actifs (Assets)*

vs

Blockchain publique

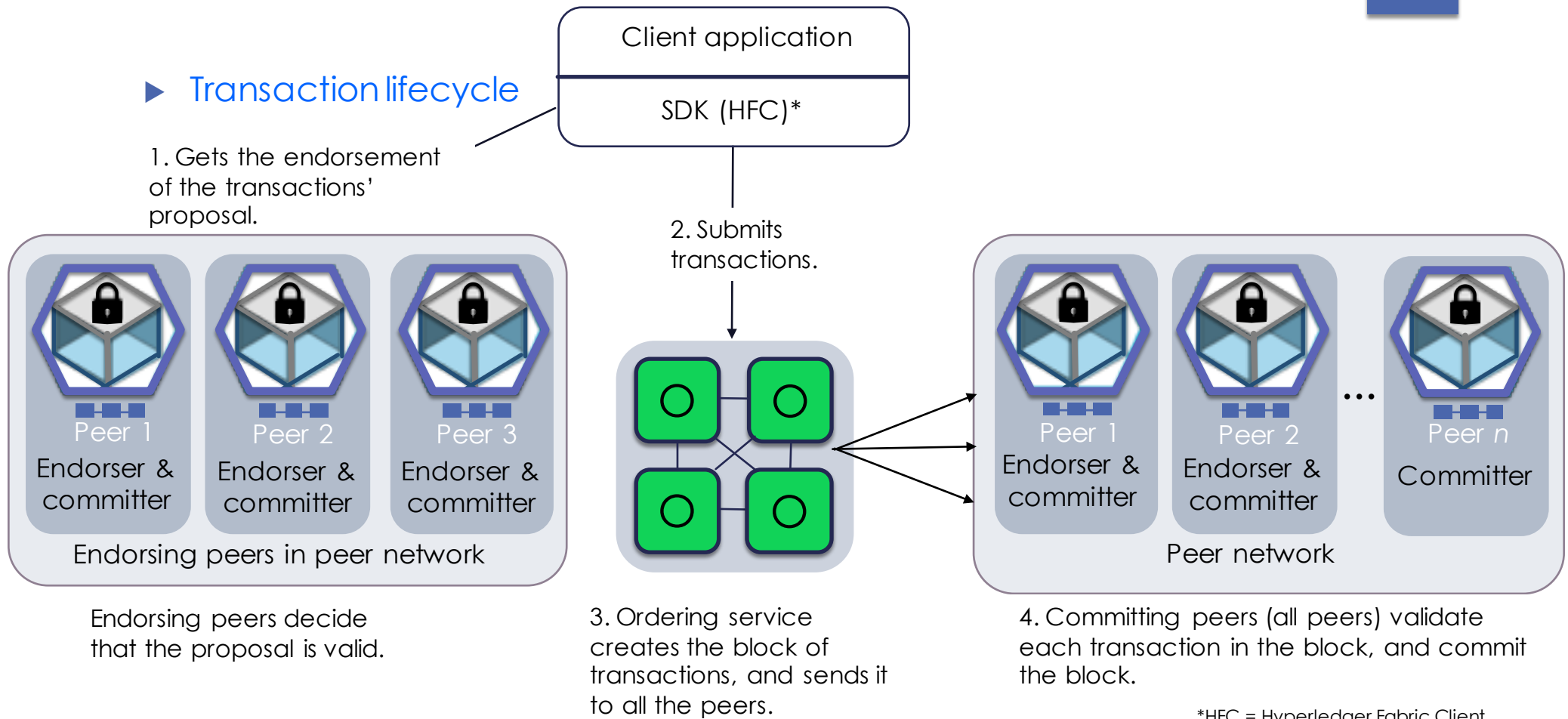
- *Anonyme*
- *Proof of Work*
- *Cryptomonnaie*

Cas de Hyperledger Fabric



Cas de Hyperledger Fabric

► Transaction lifecycle



La BLOCKCHAIN : Applications



Financial

- Trade Finance
- Cross-currency payments
- Mortgages
- Dispute Management
- Energy Trading

Public Sector

- Asset Registration
- Citizen Identity
- Medical records
- Medicine supply chain
- Voting

Retail

- Supply chain
- Loyalty programs
- Information sharing (supplier – retailer)
- Food Trust

Insurance

- Claims processing
- Risk provenance
- Asset usage history
- Claims file

Manufacturing

- Supply chain
- Product parts
- Maintenance tracking

La BLOCKCHAIN dans le monde

E-gouvernement

► **Estonie :**

- L'Estonie revendique être le 1^{er} pays à utiliser la blockchain au niveau national (e-government)
- Développe sa propre blockchain **Ksi**, axée sur la sécurité des données privées et la protection des réseaux, systèmes et données.
- Utilisée dans différents secteurs, allant des données de justice à l'identité numérique et la santé publique.

► **Sierra Leone**

- Premier pays à utiliser une BC pour **le vote électronique** dans le cadre des élections présidentielles en 2018
- Résultats en temps réels, transparence, votes infalsifiables

La BLOCKCHAIN dans le monde

E-gouvernement

- ▶ **Dubaï** : sécurisation des passeports
- ▶ **Illinois** : numérisation des actes de naissance
- ▶ **Inde** : Enregistrement des terres
- ▶ **Gibraltar, Singapour, etc** : création d'une cryptomonnaie gouvernementale réglementée

La BLOCKCHAIN dans le monde

Chaines d'approvisionnement

- ▶ IBM, Unilever, Walmart et Nestlé collaborent pour **la traçabilité des aliments**
- ▶ Everledger utilise une BC Hyperledger Fabric (IBM) pour la **traçabilité des diamants.**
- ▶ Le producteur de minerais BHP Billiton utilise une blockchain basée sur Ethereum pour **assurer la traçabilité de ses échantillons** de roches et de fluides

La BLOCKCHAIN dans le monde

- ▶ Ripple permet aux **banques de négocier entre elles** au niveau mondial sans passer par un opérateur central.
- ▶ Toyota : **Gestion des données d'assurance des voitures autonomes**
 - ▶ Stocker de façon sécurisée les données générées par la conduite automobile qui permettront ensuite de calculer les taux d'assurance

La BLOCKCHAIN dans le monde

- ▶ **BCdiploma, Blockcerts : vérifier les diplômes**
 - ▶ Stockage permanent des diplômes dans une BC
 - ▶ N'importe qui peut s'assurer de l'authenticité d'un diplôme et de l'identité de la personne à qui il a été accordé, sans avoir besoin de contacter l'établissement de formation qui l'a délivré.
- ▶ **Novembre 2019 : L'Agence Universitaire de la Francophonie & BCdiploma lancent leur service blockchain d'authentification des diplômes** → la plus grande initiative blockchain du monde universitaire
(l'université de Carthage a déjà rejoint l'initiative)

La BLOCKCHAIN : les plateformes

25

Plateforme	Type	Inventeur	Année	Consensus	Crypto-monnaie
Bitcoin	Public	Satoshi Nakamoto	2008	PoW	BTC
Ethereum	Public	Vitalik Buterin	2014	PoS	Ether (ETH)
Hyperledger Fabric	Privée	La Fondation Linux	2017	PBTF / SIEVE	Aucune
Litecoin	Public	Charles Lee	2011	Scrypt	LTC
TEZOS	Public	Tezos Foundation	2018	PoS	XTZ

Nos travaux de recherche- Contexte et Motivation

26

- Equipe de recherche **SCS-IoT : Systèmes communicants et sécurisés pour l'Internet des Objets** - Laboratoire de recherche RIADI (ENSI)

Les infrastructures de communication sans fil à la base des réseaux IoT

Défis

- Dispositifs à ressources et à capacités limitées
- Nouvelles architectures et nouveaux besoins
- Trafic dense et en milieu ouvert
- Les approches de sécurité classiques peu adaptés

Objectifs

Proposer des solutions innovantes pour sécuriser les communications dans les applications phares de l'IoT

BLOCKCHAIN, Intelligence Artificielle, théorie des jeux

Nos travaux de recherche - Contributions et projets en cours

27

1. Sécurité des communications dans les réseaux de transport intelligents

Problématique

- ▶ Les réseaux de transport intelligents sont de plus en plus répandus avec plusieurs services pour la sécurité routière, la localisation et les services aux passagers
 - ▶ Communications intra-véhicules
 - ▶ Communications inter-véhicules et véhicules-infrastructure
- ▶ **Architecture complexe et divers contraintes (densité dans les villes, mobilité accrue, etc.) → vulnérabilité accrue et besoin de sécurité à plusieurs échelles**

Approches

- ▶ Etude et proposition de nouvelles **méthodes de sécurité basées sur l'intelligence artificielle** pour la détection des anomalies dans les réseaux CAN
- ▶ Etude et proposition de méthode intelligentes pour les communications dans les réseaux véhiculaires V2V et V2I
- ▶ Intégration de la **Blockchain** dans les architectures de communication et de services Edge-ITS

Nos travaux de recherche - Contributions et projets en cours

28

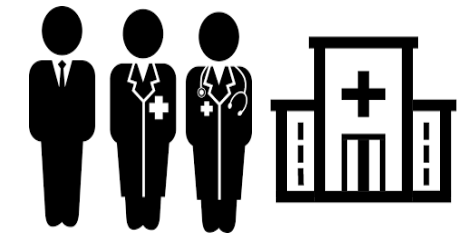
2. Blockchain pour la e-santé

Problématique

- ▶ Les données médicales sont des données sensibles
- ▶ Nécessité de garantir le respect de la vie privée
- ▶ Besoin d'un contrôle d'accès lors du transit des données médicales entre les différents acteurs et parties prenantes d'un système médical national

Approches

- ▶ **Proposer une architecture distribuée pour la gestion des données médicales à l'échelle national**
- ▶ **Système de contrôle d'accès basé sur une Blockchain**



Healthcare provider



Patient



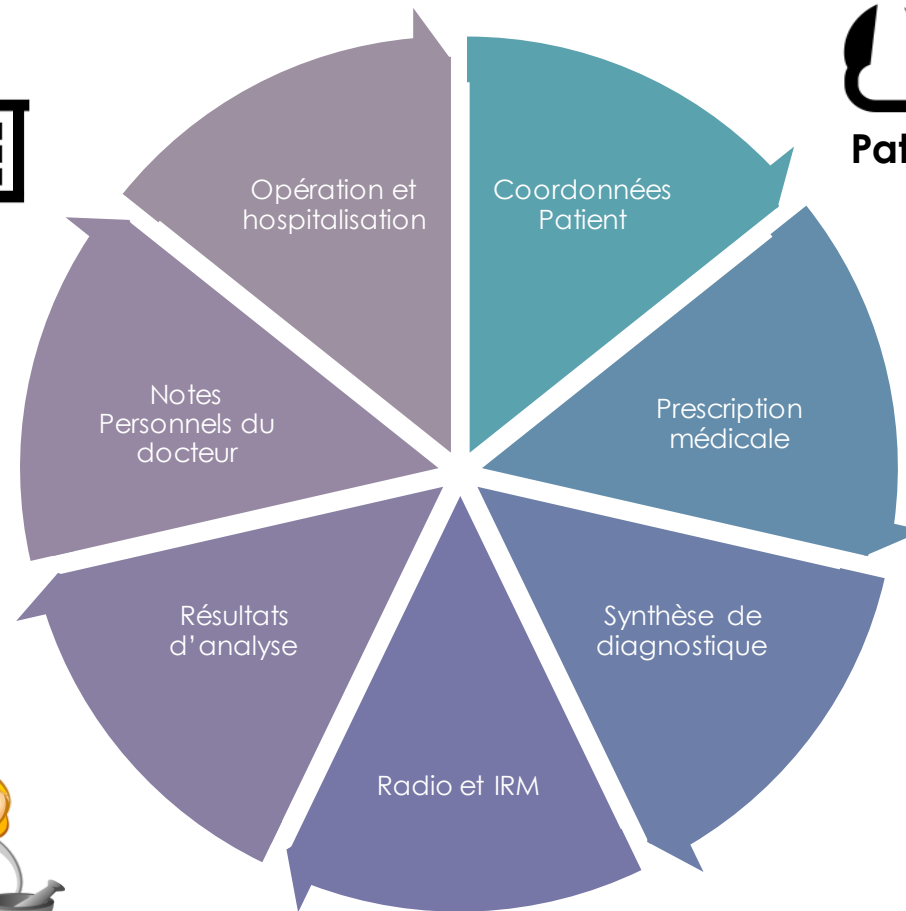
Research institutes

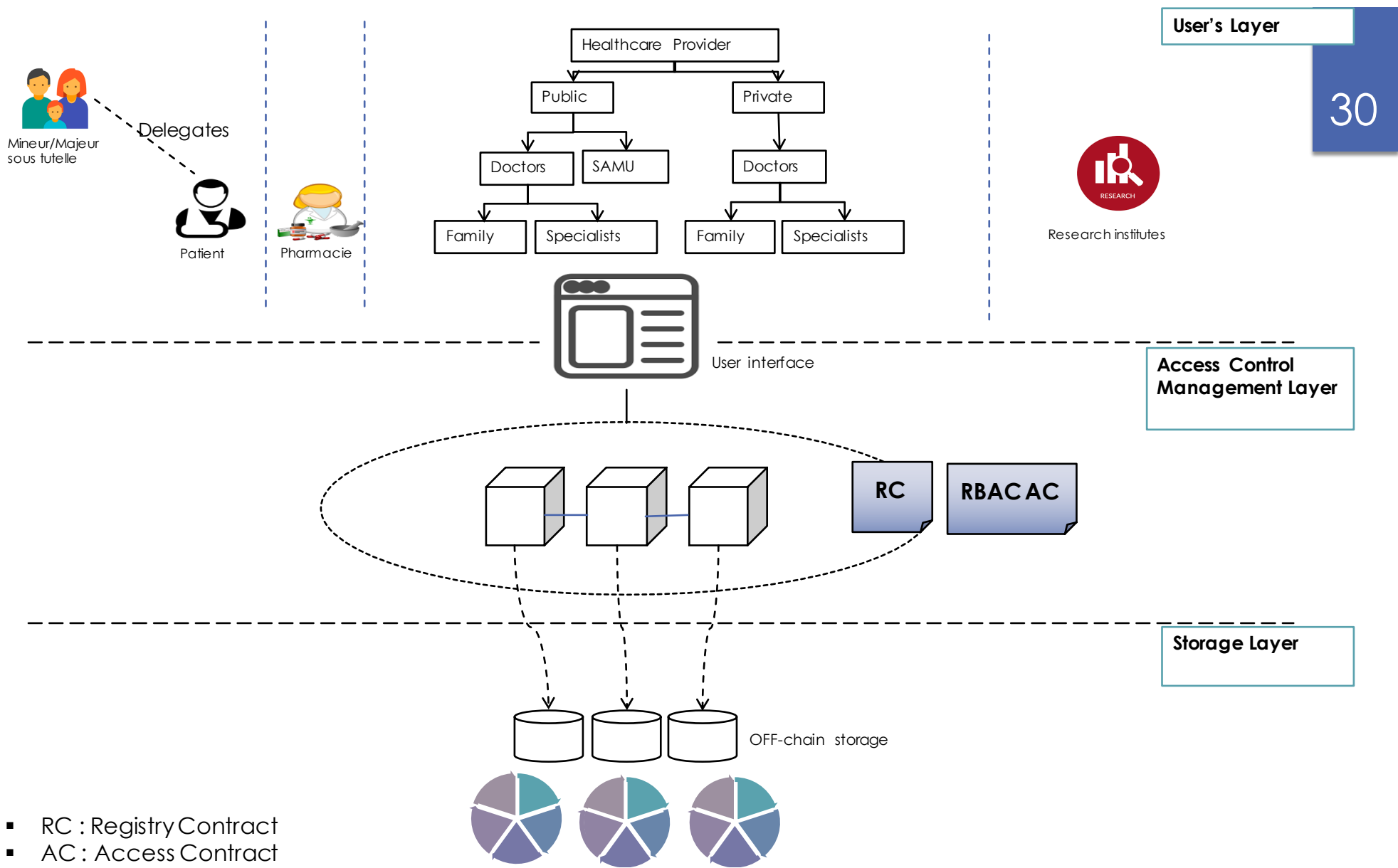


Pharmacie



Emergency Staff





Nos travaux de recherche - Valorisation et impact

- ▶ Collaborations internationales
 - ▶ Laboratoire de recherche LABRI, Université de Bordeaux
 - ▶ Laboratoire CREtice, Université Technologique de Troyes
 - ▶ Laboratoire LISSI, Université Paris-Est Créteil

- ▶ Impact en terme de diplomation
 - ▶ 1 thèse soutenue + 1 thèse en cours
 - ▶ 4 Master de recherche (dont 2 soutenus)

- ▶ Dissémination
 - ▶ Plusieurs publications scientifiques dans des revues et des conférences de haut niveau
 - ▶ Organisation de la 1^{ère} école d'automne sur la Blockchain, Novembre 2019.



Merci pour votre attention
Questions ?