Cybersécurité - Cours 6: La blockchain

SIO - Bloc 3 - SMDSI

M. SPINA

Sommaire

1) Mise en contexte
2) Exemple d’une transaction classique
3) Naissance d’un système révolutionnaire
4) Evolution des transactions
5) Différents types de réseaux
6) Les avantages de la blockchain
7) Le Bitcoin
8) Les outils
9) La chaîne de blocs
10) Fonctionnement et définitions

Mise en contexte: les transactions

Depuis toujours, des instruments dignes de confiance ont été développés pour faciliter l'échange de biens et pour protéger à la fois acheteurs et vendeurs:

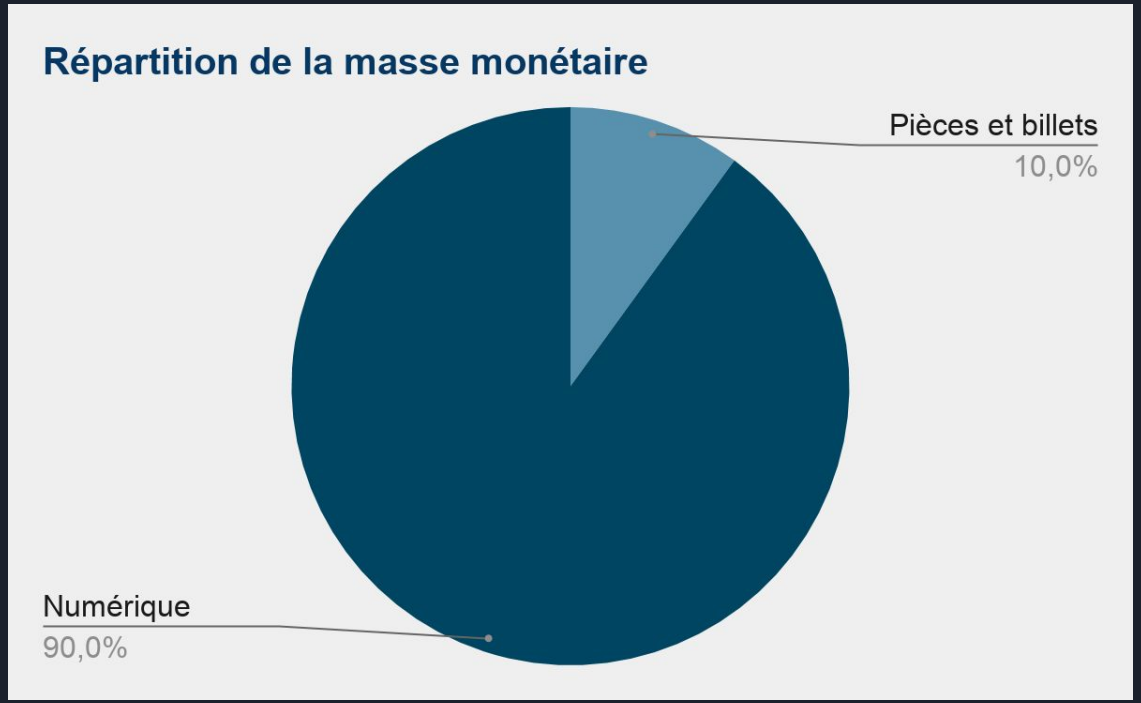
- les pièces de monnaie
- les billets

Mise en contexte: les transactions

Grâce à des innovations importantes, les transactions ont gagné en **commodité**, en **vitesse** et en **efficacité**, jusqu'à réduire, et même éliminer, toute distance entre acheteurs et vendeurs:

- Internet
- les systèmes à cartes de crédit
- les technologies mobiles

Mise en contexte: les transactions



Mise en contexte: Systèmes existants

Les moyens de paiement évoluent et se multiplient. Cependant, certains d'entre eux présentent encore **quelques inconvénients**:

- Les liquidités sont utiles pour les transactions locales à **faible montant**
- Le **délai d'attente** concernant une transaction peut être long
- La nécessité d'une validation par des **tiers de confiance ou intermédiaires**
- La **fraude et les cyberattaques** sont toujours présentes

Exemple d’une transaction classique

Tiers de confiance

=

Réseau centralisé

Interroge la base de données

Inscrit dans le registre

Exemple d’une transaction classique

Inconvénients de l’intervention d’un tiers de confiance:

- **Délai d’attente** lors de transactions à montant élevé
- **Frais annexes** liés à la gestion des comptes
- Monopolisation des **droits et autorisations** sur les comptes
- Obligation de **faire confiance** aux banques
- Rendement très faible de votre épargne

Naissance d’un système révolutionnaire

C’est pourquoi, des développeurs ont cherché à créer un système permettant de pallier aux différents inconvénients des systèmes existants.

Ainsi, ce système permettrait d’allier:

- rapidité et efficacité
- rentabilité
- fiabilité
- sécurité

dans la réalisation et l’enregistrement des transactions financières.

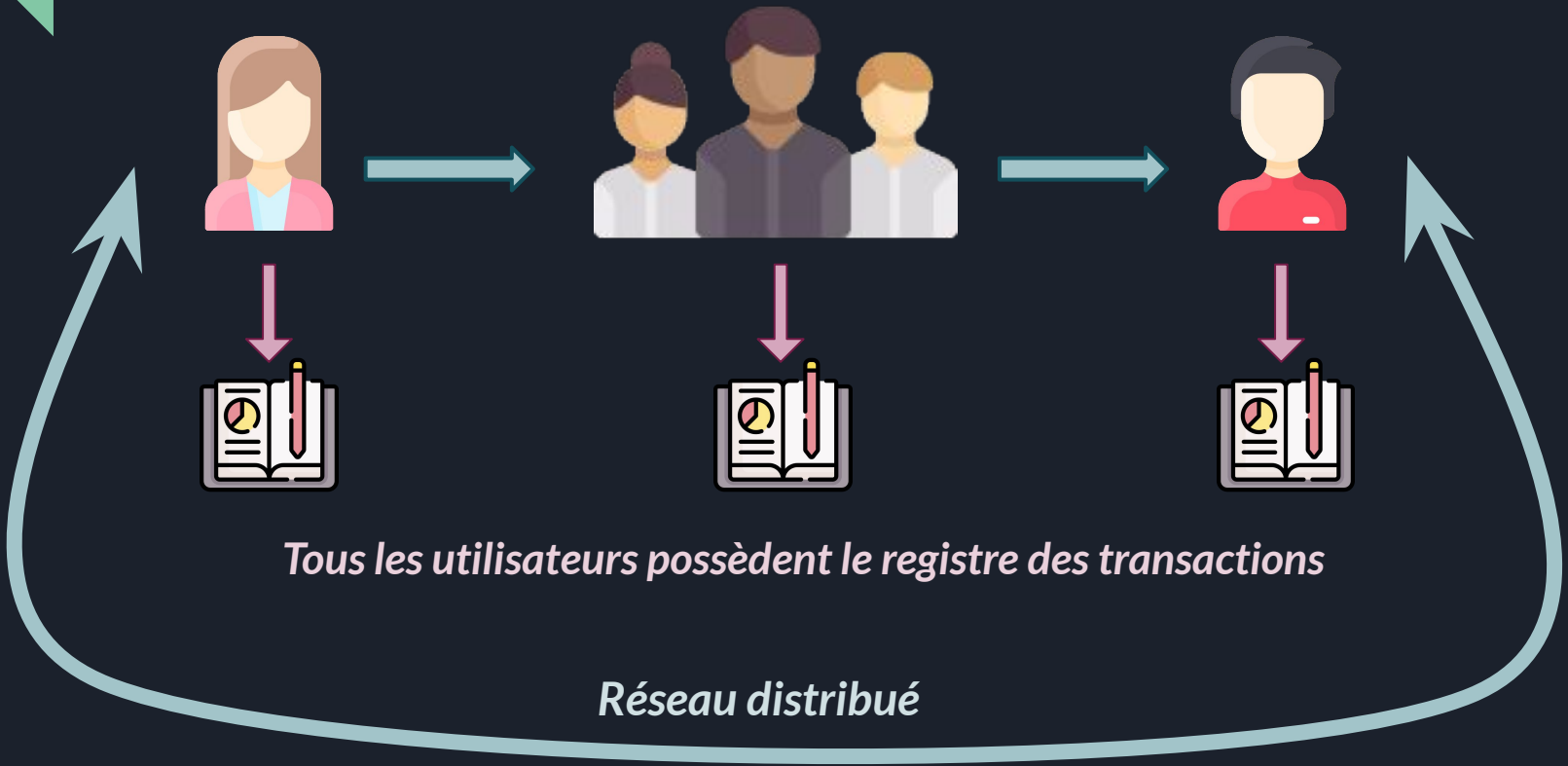
Evolution d’une transaction classique

Tiers a[illegible]nfiance

Interroge la base de données

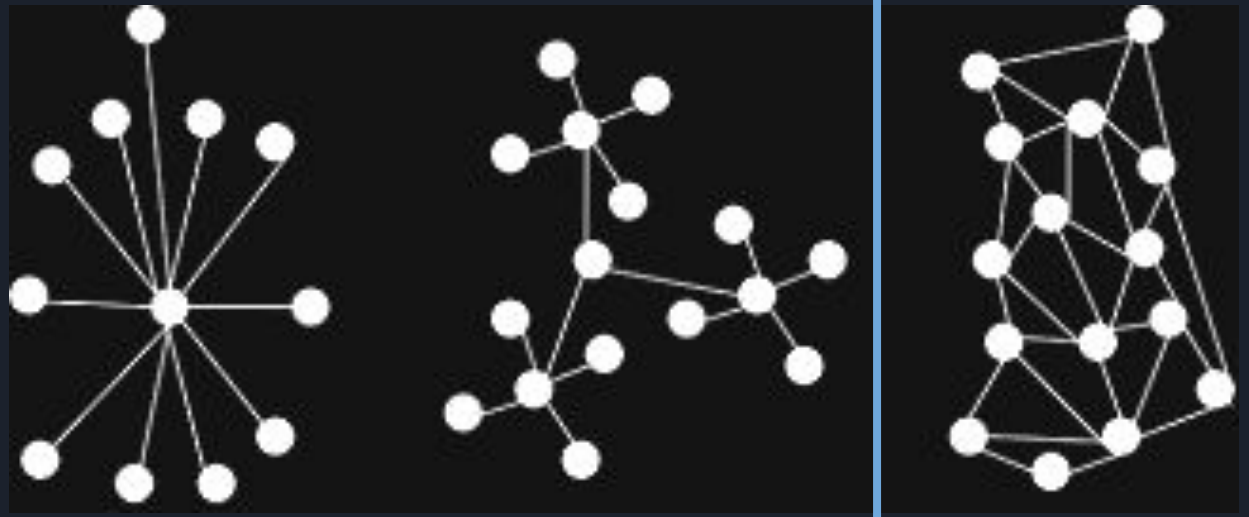
Inscrit dans le registre

Evolution d’une transaction classique



Différents types de réseau

Réseau blockchain



Réseau centralisé

Réseau décentralisé

Réseau distribué

Les avantages de la blockchain

Sécurité absolue

- Transactions publiques mais anonymes
- Transactions vérifiables par tous
- Transactions enregistrées & irréversibles
- Transactions infalsifiables

Transparence totale

- Sans tiers de confiance
- Aucune fraude possible
- Protégé contre la fraude de la double-dépense

Cas d’utilisation: le Bitcoin

→ **crypto-monnaie**, lancée en 2009 par une ou plusieurs personnes dont l’identité reste mystérieuse, puisqu’elle n’est connue que par un pseudonyme : Satoshi Nakamoto.

→ une des solutions développées pour répondre aux problèmes de **complexité, de vulnérabilité, d’inefficacité et de coût des systèmes de transactions existants**

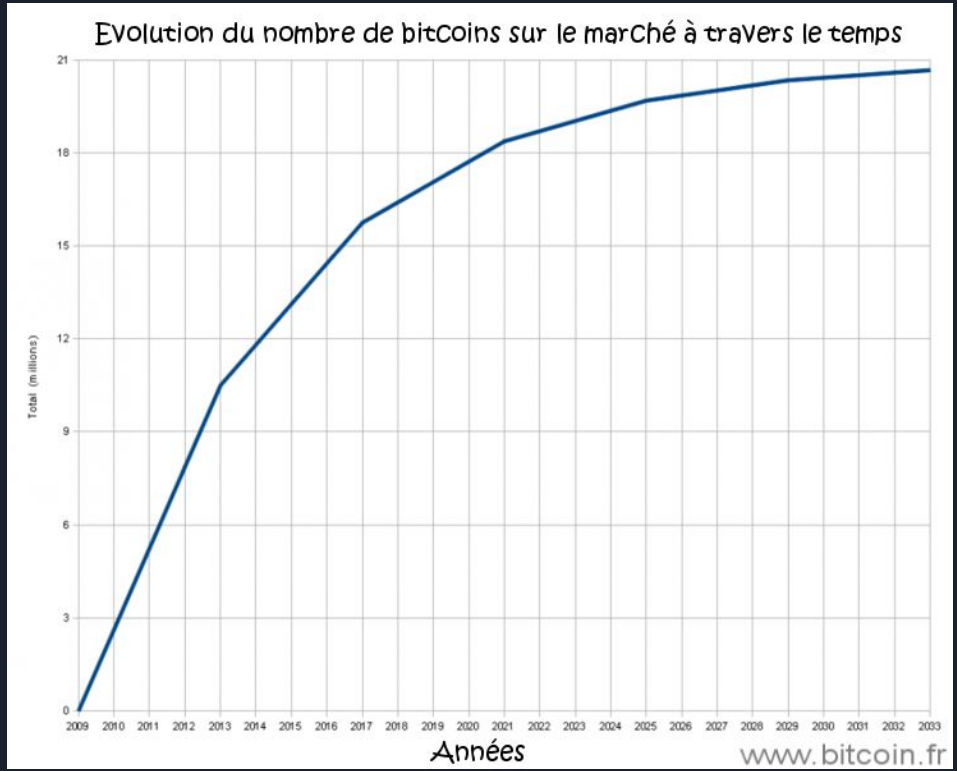
Evolution du Bitcoin

Nb Total de Bitcoin disponibles:
21 000 000

Nb de Bitcoin en circulation:
18 871 625

Nouveau Bitcoin/jour:
900

Valeur du Bitcoin:
1 BTC = 35 500€



Les outils du Bitcoin

1) Le chiffrement asymétrique
   → **Authentification** au système

2) La fonction de hachage
   → Marquer une **empreinte** sur les transactions

3) La chaîne de blocs
   → **Partager le registre** des transactions

Définition de la blockchain

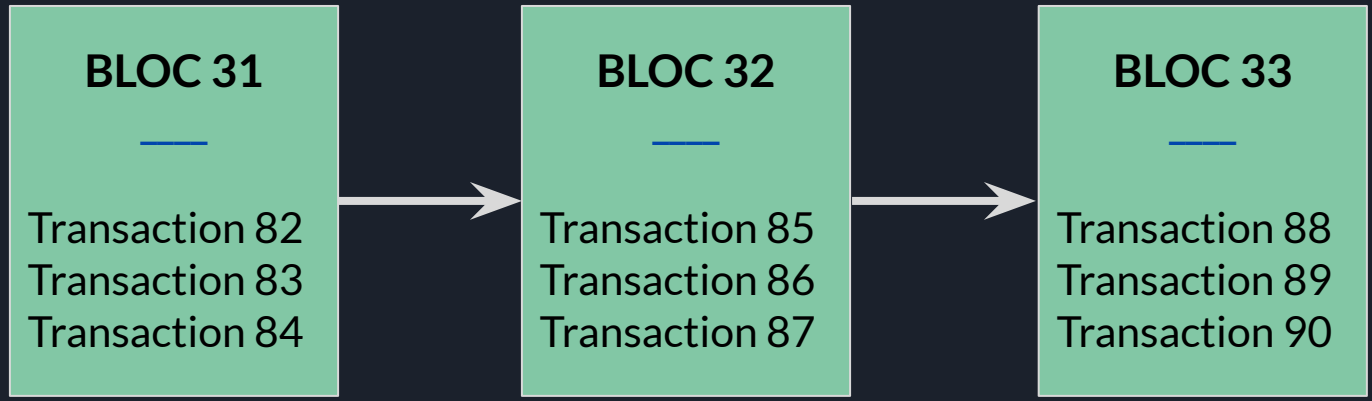
La Blockchain est **un registre partagé et distribué** destiné à **faciliter le processus d'enregistrement des transactions** et de suivi des actifs dans un réseau d'entreprises.

Un actif peut être un bien **tangible** (maison, voiture, liquidités, terrain), ou **intangible**, par exemple des éléments de propriété intellectuelle comme les brevets, les droits d'auteur ou les marques.

Un réseau Blockchain permet de **suivre et d'échanger** pratiquement tout bien possédant une certaine valeur en réduisant les risques et en diminuant les coûts pour tous les interlocuteurs concernés.

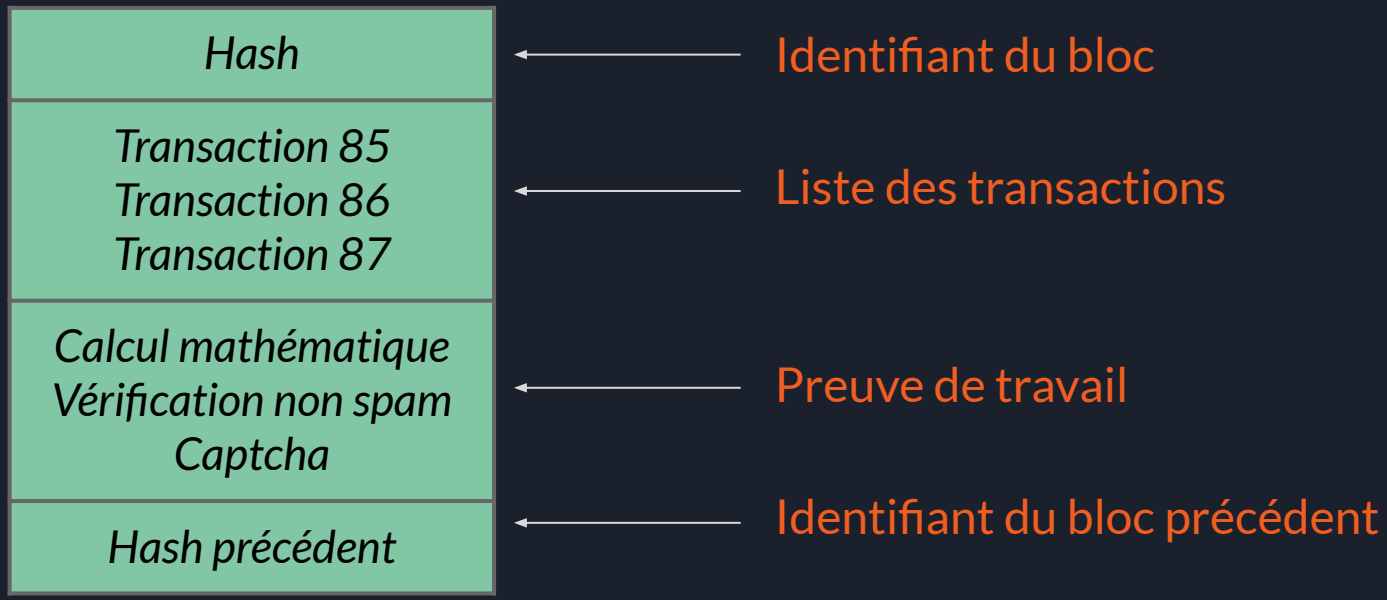
Fonctionnement de la blockchain

Un bloc contient une liste des transactions



L'ensemble des blocs forment une chaîne de blocs

Contenu d’un bloc



Qu’est-ce qu’une preuve de travail ?

La preuve de travail (en anglais ***proof-of-work*** ou ***PoW***) est un **processus de vérification automatisé**. Il doit être créé de façon à ce qu’il ne soit pas nécessaire de prendre du temps pour vérifier qu’il corresponde aux critères demandées.

- ➔ plus besoin de prendre du temps pour vérifier des choses
- ➔ limiter les spam et les dénis de service
- ➔ inconvénient: coût de production et d’énergie

PoW: Exemple 1

- **Hashcash**, solution créée en 1997 par Adam Baker pour prévenir contre les spams.

Basée sur une fonction de hachage, elle se présente sous la forme d'un plugin relié au client mail qui ajoute des timbres hashcash aux mails.

```
From: Quelqu'un <test@test.invalid>
To: Adam Back <adam@cyberspace.org>
Subject: test hashcash
Date: Jeu, 26 Février 2021 11:59:59 +0000
X-Hashcash:
0:030626:adam@cyberspace.org:6470e06d773e05a8
```

PoW: Exemple 2

- **Captcha**: développé en 2000 à l'université Carnegie-Mellon, solution permettant de différencier de manière automatisée un utilisateur humain d'un ordinateur.

La technique demande à l'utilisateur de recopier des lettres ou de reconnaître des images afin de prouver qu'il n'est pas un bot.