

Nouveaux Modèles économiques

Chapitre 2
La smart économie

Plan général du cours

1. Perspectives de long terme, croissance et inégalités

2. La smart économie

3. Commerce international, anciens modèles

4. Commerce des tâches et chaînes de valeur internationales

5. Marchés et concurrences, concurrence et monopole

6. Marchés et concurrences, concurrences imparfaites

7. Innovations et diversité

8. L'économie des plateformes

9. Politiques de la concurrence

Plan de la session

1. Qu'est-ce que la monnaie ?
2. Le blockchain et les cryptomonnaies
3. Smart contracts
4. Quelques perspectives sur l'AI

Plan de la session

1. Qu'est-ce que la monnaie ?

2. Le blockchain et les cryptomonnaies

3. Smart contracts

4. Quelques perspectives sur l'AI

Définition classique de la monnaie

Unité de compte

Marque la valeur relative des biens

Sert de base aux calculs économiques

Réserve de valeur

Permet l'épargne, i.e. le transfert temporel de richesse

À travers la thésaurisation

À travers le circuit du capital (unité de compte, échanges)

Intermédiaire des échanges

Facilite la pratique décentralisée des échanges

Unité de compte des dettes accumulées (apurement)

Le mythe du troc

Mais dans les commencements de l'établissement de la division du travail, cette faculté d'échanger dut éprouver de fréquents embarras dans ses opérations. Un homme, je suppose, a plus d'une certaine denrée qu'il ne lui en faut, tandis qu'un autre en manque. En conséquence, le premier serait bien aise d'échanger une partie de ce superflu, et le dernier ne demanderait pas mieux que de l'acheter. Mais si par malheur celui-ci ne possède rien dont l'autre ait besoin, il ne pourra pas se faire d'échange entre eux. Le boucher a dans sa boutique plus de viande qu'il n'en peut consommer, le brasseur et le boulanger en achèteraient volontiers une partie, mais ils n'ont pas autre chose à offrir en échange que les différentes denrées de leur négoce, et le boucher est déjà pourvu de tout le pain et de toute la bière dont il a besoin pour le moment. Dans ce cas-là, il ne peut y avoir lieu entre eux à un échange.

Le mythe du troc

Pour éviter les inconvénients de cette situation, tout homme prévoyant, dans chacune des périodes de la société qui suivirent le premier établissement de la division du travail, dut naturellement tâcher de s'arranger pour avoir par-devers lui, dans tous les temps, outre le produit particulier de sa propre industrie, une certaine quantité de quelque marchandise qui fût, selon lui, de nature à convenir à tant de monde, que peu de gens fussent disposés à la refuser en échange du produit de leur industrie. Il est vraisemblable qu'on songea, pour cette nécessité, à différentes denrées qui furent successivement employées. Dans les âges barbares, on dit que le bétail fut l'instrument ordinaire du commerce; et quoique, ce dût être un des moins commodes, cependant, dans les anciens temps, nous trouvons souvent les choses évaluées par le nombre de bestiaux donnés en échange pour les obtenir.

Adam Smith (1776) Recherche sur la nature et les causes de la richesse des nations

Le mythe du troc

On dit qu'en Abyssinie le sel est l'instrument ordinaire du commerce et des échanges; dans quelques contrées de la côte de l'Inde, c'est une espèce de coquillage; à Terre-Neuve, c'est de la morue sèche; en Virginie, du tabac; (...).

Cependant, des raisons irrésistibles semblent, dans tous les pays, avoir déterminé les hommes à adopter les métaux pour cet usage, par préférence à toute autre denrée. Les métaux non seulement ont l'avantage de pouvoir se garder avec aussi peu de déchet que quelque autre denrée que ce soit, aucune n'étant moins périssable qu'eux, mais encore ils peuvent se diviser sans perte en autant de parties qu'on veut, et ces parties, à l'aide de la fusion, peuvent être de nouveau réunies en masse ; qualité que ne possède aucune autre denrée aussi durable qu'eux, et qui, plus que toute autre qualité, en fait les instruments les plus propres au commerce et à la circulation.

Adam Smith (1776) Recherche sur la nature et les causes de la richesse des nations

Crédit et confiance

Le mythe de la création de la monnaie

Autarcie → division du travail + troc → monnaie → crédit

Mythe contredit par les études historiques

David Graeber (2011) *Debt: the first 5000 years*, Melville House Publishing

Exemples d'Adam Smith au mieux anecdotique

Réalité des échanges par crédit avant la monnaie

Boeuf et bestiaux : unité de compte et non intermédiaire

Élargissement des échanges et confiance

Communauté restreinte, rapports récurrents, contrôle social
→ *possibilité de confiance et donc de crédit*

Commerce élargi, nécessité de matérialiser les transactions
→ *troc ou intermédiaire des échanges (or, monnaie)*

Monnaie, confiance et pouvoir

Contrôle de la monnaie par les pouvoirs politiques

Assurer la crédibilité de l'intermédiaire des échanges

Certification du contenu de la pièce

Loi obligeant à l'accepter à la valeur faciale

Contrôler les échanges économiques et seigneurage

Monnaie métallique : valeur faciale < contenu réel

Monnaie de crédit : création de monnaie

Création de monnaie et inflation

Monnaie métallique : risque de réalignement sur contenu

Monnaie de crédit : effet richesse et demande ↑

→ importance des causes : capacités productives ou consommation

La question de l'annulation partielle de la dette

Définition pratique de la monnaie

Définition de la monnaie

La monnaie est un moyen d'échange comprenant les billets de banque, les dépôts bancaires ou tout autre élément qui puisse être utilisé comme moyen de paiement, et qui est accepté parce que d'autres peuvent l'utiliser aux mêmes fins.

La monnaie peut (doit) être créée

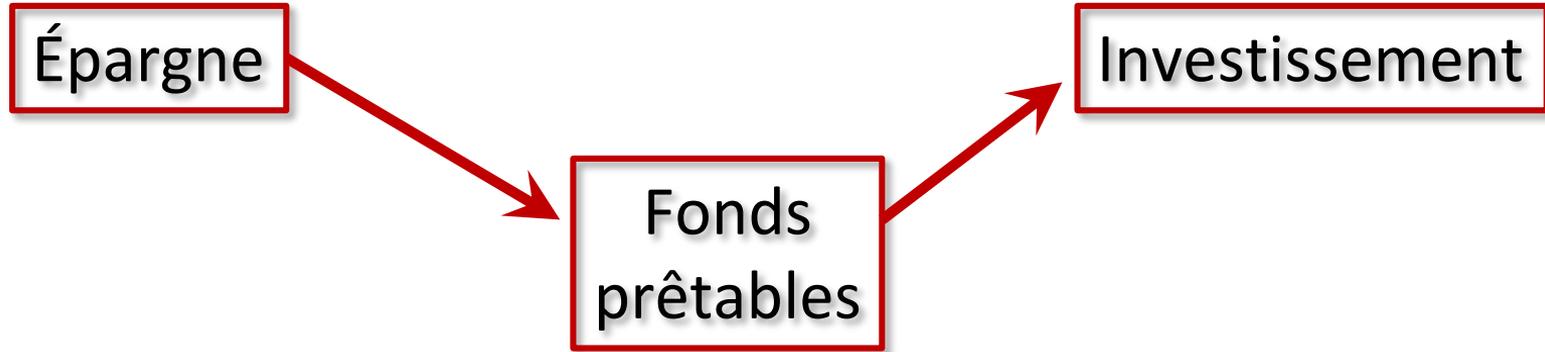
Une richesse matérielle peut servir de monnaie (métaux)

Mais aujourd'hui il s'agit d'un titre immatériel

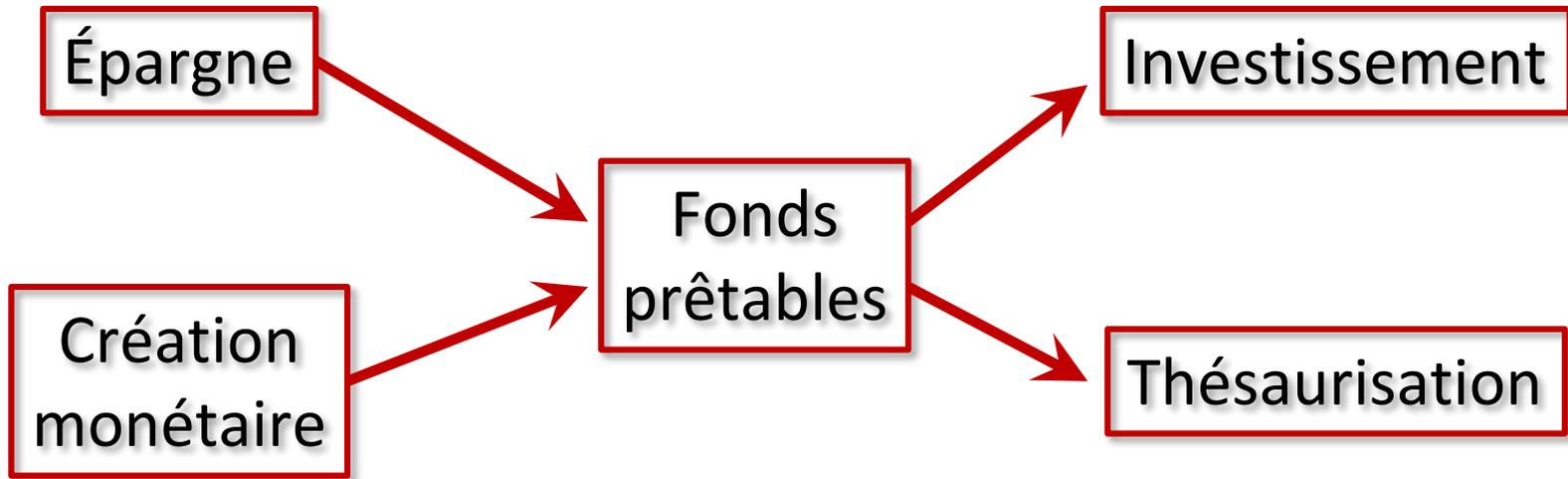
C'est une relation de confiance partagée (ou imposée)

→ est créée par les banques centrales ou commerciales

Circuit de financement



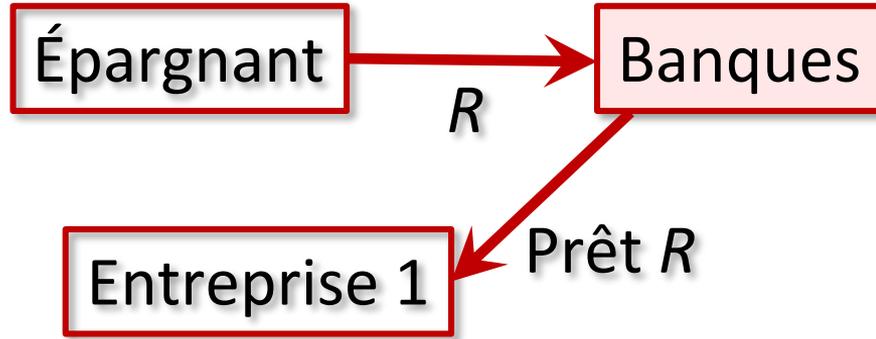
Circuit de financement



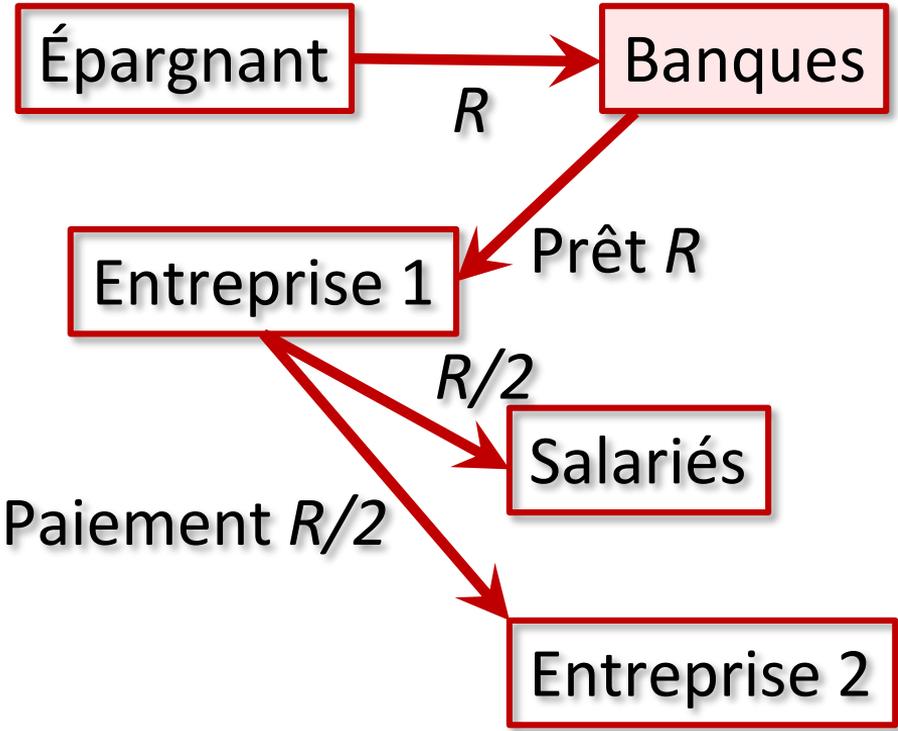
Création monétaire privée



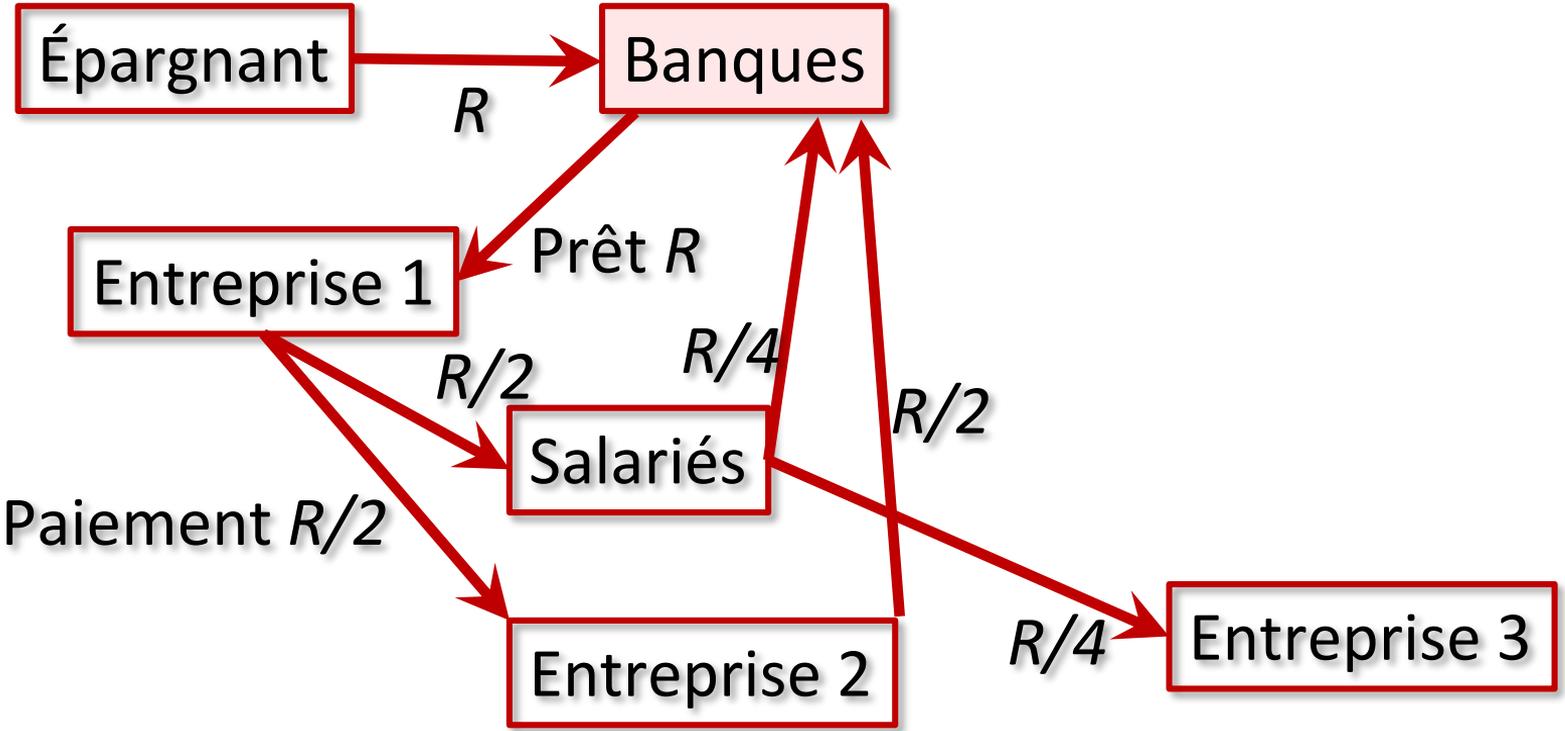
Création monétaire privée



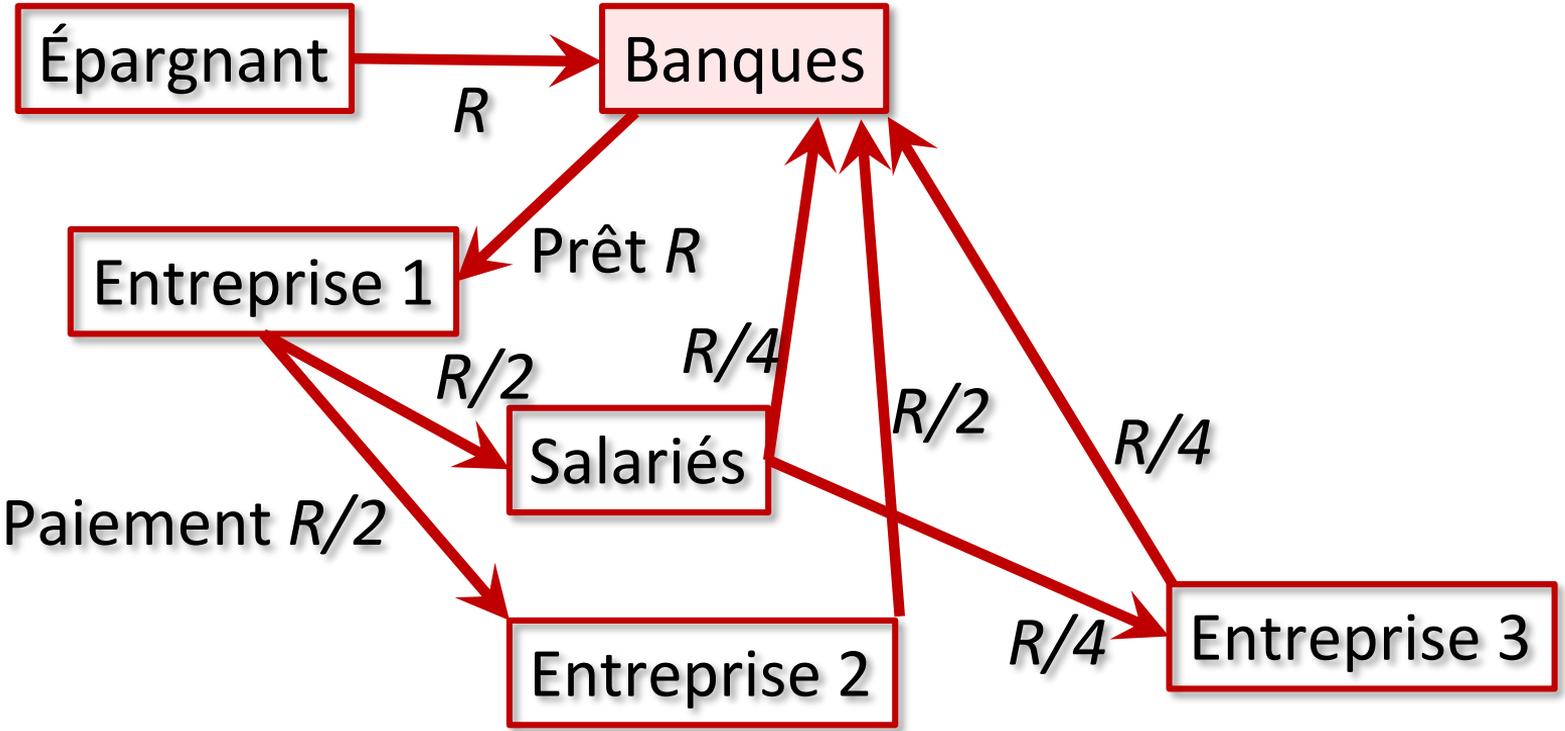
Création monétaire privée



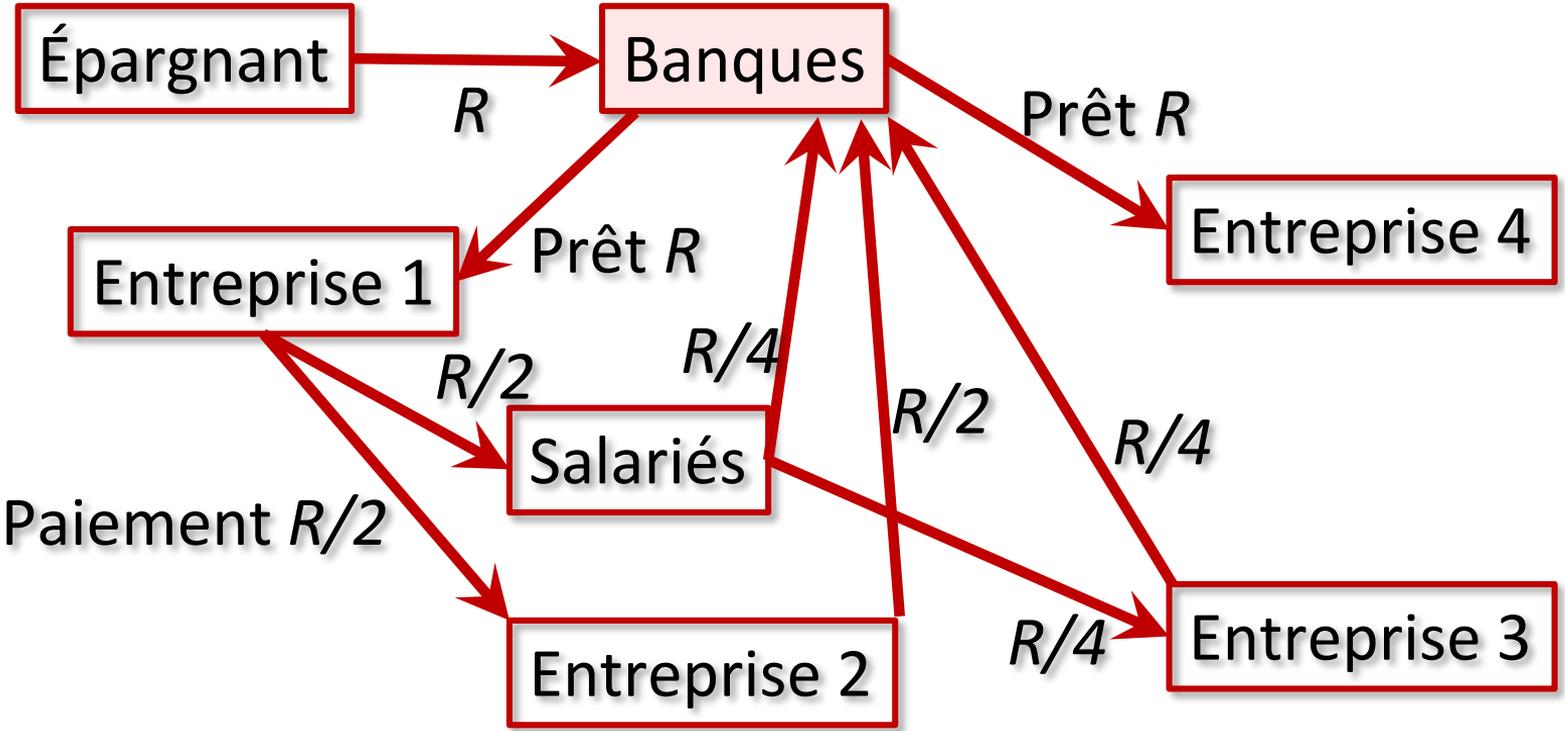
Création monétaire privée



Création monétaire privée



Création monétaire privée



Monnaie privée, monnaie centrale

Organisation actuelle du système bancaire

Création monétaire par les banques commerciales

Contrôlées par les banques centrales

Contraintes sur les banques commerciales (réserves)

Incitation des banques commerciales (refinancement)

+ Politiques monétaires non conventionnelles

Possibilité de monétiser les dettes

La confiance repose sur des personnes morales

Banques centrales

Banques commerciales

Entreprises de transactions (carte bleue, visa, mastercard...)

Certification d'une transaction

Principe du cryptage RSA

Clef privée A \rightarrow permet de calculer clef publique A'

Mais A est très difficile à retrouver depuis A'

En fait A est deux nombres premiers et A' leur produit

Message M , si code avec A' : $C^{A'} = f(M, A') \rightarrow M = f(C^{A'}, A)$

Message M , si code avec A : $C^A = f(M, A) \rightarrow M = f(C^A, A')$

Utilisations pour authentifier des transactions

Banque possède (A, A') et transmet A' aux terminaux

Sur la carte : en privé \rightarrow un jeu de clefs (B, B')

en public \rightarrow n° de compte, $f(B', A)$

Terminal décode B' (avec A') et code $C^{B'} = f(M, B')$

\rightarrow *Seule vraie carte peut répondre $M = f(C^{A'}, A)$*

\rightarrow *Besoin de A pour construire une carte qui marche*

Plan de la session

1. Qu'est-ce que la monnaie ?

2. Le blockchain et les cryptomonnaies

3. Smart contracts

4. Quelques perspectives sur l'AI

Idée générale du Bitcoin

Les objectifs du bitcoin

Créer un intermédiaire des échanges (de fait une monnaie)

Sans tier de confiance ni personne morale dominante

→ *décentralisation complète de la confiance*

Mais qui soit sécurisée

Assurer que les payeurs sont solvables dans la monnaie

Assurer que les transactions sont réelles et voulues

Création de la crédibilité

Transparence totale de la création monétaire

Initialisation à l'intérieur d'une communauté → confiance

Processus progressif d'extension conservant la crédibilité

Technologie sous-jacente

Blockchain : registre public sécurisé

Registre public → information transparente et indélébile
On ne peut payer qu'avec un compte solvable
Mécanisme sécurisé et décentralisé d'ajouts de maillons

Sécurisation des transactions

Le numéro de compte est la clef publique A'
 A' annonce transférer $x\text{€}$ du compte A' au compte B'
Et certifie en codant le message d'authentification $C = f(M, A)$
Problème : vérifier que $f(C, A') = M$ et ajouter à la chaîne
→ *multiplicité et tirage aléatoire des vérificateurs*

Tirer au sort les registraires

Mécanisme du *proof of work*

Tout le monde peut être certificateur → décentralisation
Contrôle du nombre de certificateurs par *proof of work*
Calculs nécessaires pour proposer un nouveau maillon
Éviter les fausses IPs : ~~1 IP = 1 voix~~ → 1CPU = 1 voix
Coût énergétique réel pour proposer un block
Payée par de la création monétaire (incitation)

Permet de gérer la création monétaire

Génération d'un nouveau block toutes les 10 minutes
Flux de paiement en ฿ prédéterminé : transparence création
Adaptation automatique de la difficulté du *Proof of Work*

Limites des cryptomonnaies

Limites liées au *proof of work*

Succès de la monnaie → haute valeur du minage
→ mineurs ↑ → coût énergétique ↑
→ *graphique*

Concentration des investissements réels dans les mines
→ *majorité des CPU = majorité des voix (sécurité ?)* → *graphique*

Existe protocoles moins consommateurs (décentralisation ↓)

Recentralisation du système

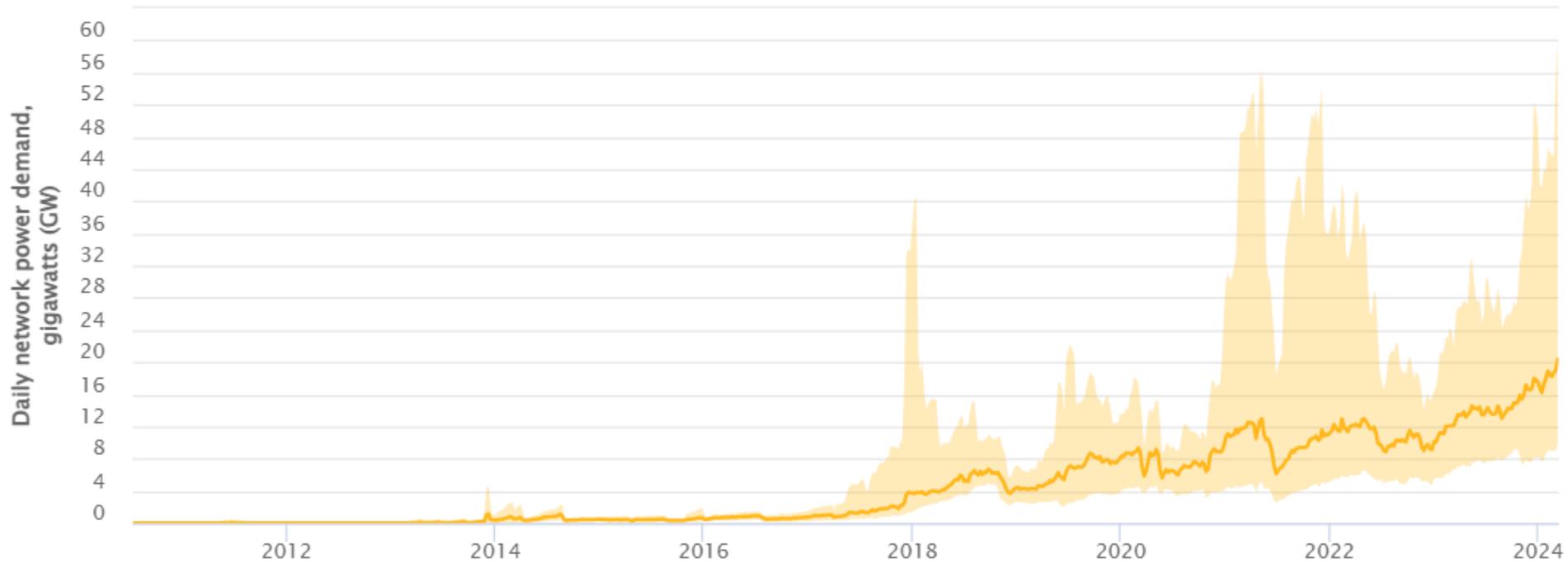
Accès au réseau par des intermédiaires monnaie ↔ bitcoin

Certification de solvabilité des comptes, de non criminalité

→ Création d'agence de vérification des comptes

→ Réinstallation d'organismes certificateurs centralisés

Consommation électrique



Limites des cryptomonnaies

Limites liées au *proof of work*

Succès de la monnaie → haute valeur du minage
→ mineurs ↑ → coût énergétique ↑
→ *graphique*

Concentration des investissements réels dans les mines
→ *majorité des CPU = majorité des voix (sécurité ?)* → *graphique*

Existe protocoles moins consommateurs (décentralisation ↓)

Recentralisation du système

Accès au réseau par des intermédiaires monnaie ↔ bitcoin

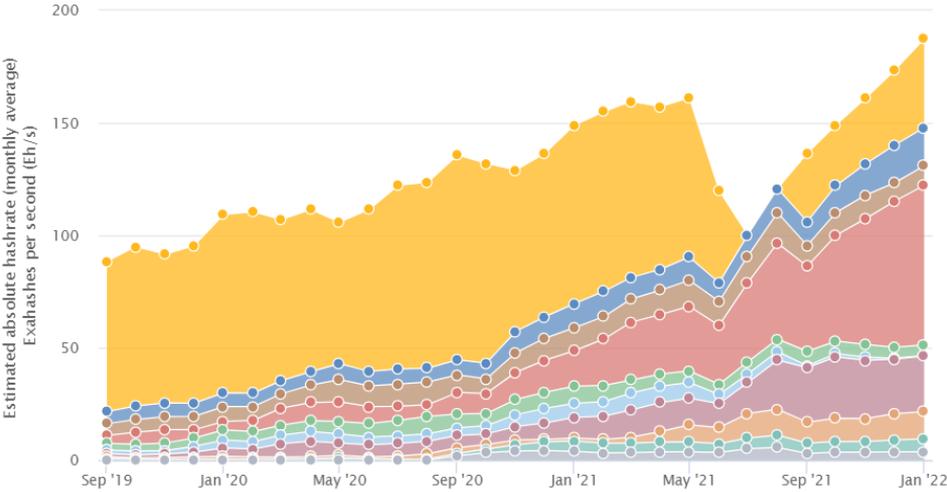
Certification de solvabilité des comptes, de non criminalité

→ Création d'agence de vérification des comptes

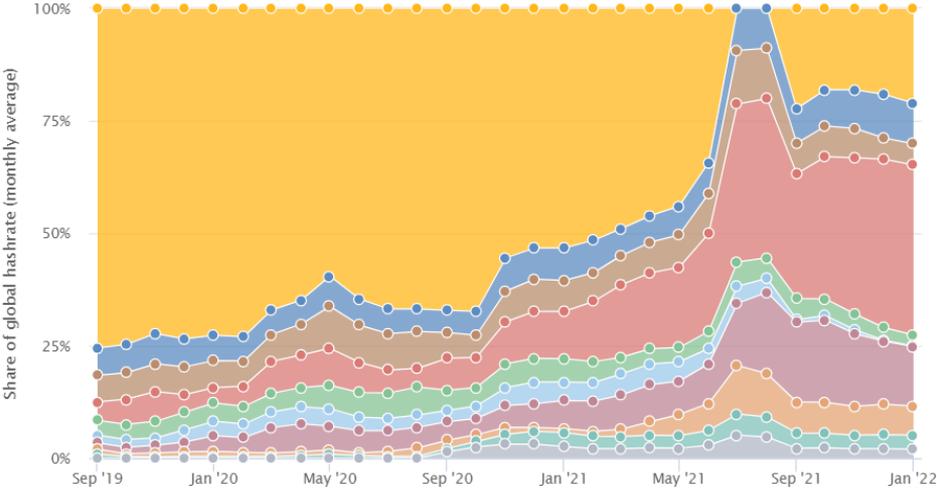
→ Réinstallation d'organismes certificateurs centralisés

Centralisation du minage

Evolution of network hashrate



Evolution of country share



- Mainland China
- Other
- Russian Federation
- United States
- Malaysia
- Iran, Islamic Rep.
- Kazakhstan
- Canada
- Germany *
- Ireland *

- Mainland China
- Other
- Russian Federation
- United States
- Malaysia
- Iran, Islamic Rep.
- Kazakhstan
- Canada
- Germany *
- Ireland *

Limites des cryptomonnaies

Limites liées au *proof of work*

Succès de la monnaie → haute valeur du minage
→ mineurs ↑ → coût énergétique ↑
→ *graphique*

Concentration des investissements réels dans les mines
→ *majorité des CPU = majorité des voix (sécurité ?)* → *graphique*

Existe protocoles moins consommateurs (décentralisation ↓)

Recentralisation du système

Accès au réseau par des intermédiaires monnaie ↔ bitcoin

Certification de solvabilité des comptes, de non criminalité

→ Création d'agence de vérification des comptes

→ Réinstallation d'organismes certificateurs centralisés

Plan de la session

1. Qu'est-ce que la monnaie ?
2. Le blockchain et les cryptomonnaies
- 3. Smart contracts***
4. Quelques perspectives sur l'AI

Principes généraux

Principes de la blockchain

Stockage de données indélébiles sur nœuds multiples
Assurant la validité (consensus)
Et la chronologie (pas d'insertion entre block)

Smart contracts

Programmes autonomes codés sur une blockchain
Exécution automatique de tout ou partie d'un contrat
Selon des conditions préprogrammées
En lien avec des informations sur les nouveaux block
Par exemple : sinistre → paiement assurantiel

Permissions sur la blockchain

	Lecture restreinte	Lecture ouverte
Écriture restreinte	Privée	Gouvernementale
Écriture ouverte	Surveillance	Publique

Privée : Everledger, la blockchain des diamantaires
Transactions et caractéristiques des diamants

Publique : Bitcoin et autres cryptomonnaies

Gouvern^{ta}le : Cadastres, registre introduction bourse Delaware

Surveillance : Suivi d'évènements, de sinistres
Exécution automatique de paiements d'assurance

Avantages/inconvénients

	Blockchains privées	Blockchains publiques
Gouvernance	+	-
Externalités indirectes (plateformes multi-versants)	0/+	+
Externalités de sécurité	0	+
Externalités négatives de minage	0	-
Efficacité de la preuve	+	-
Externalité de sécurisation	0	+
Responsabilité	+	-
Ouverture et interopérabilité	-	+
Confidentialité	+	0
Monétisation	+	0

La blockchain dans la finance

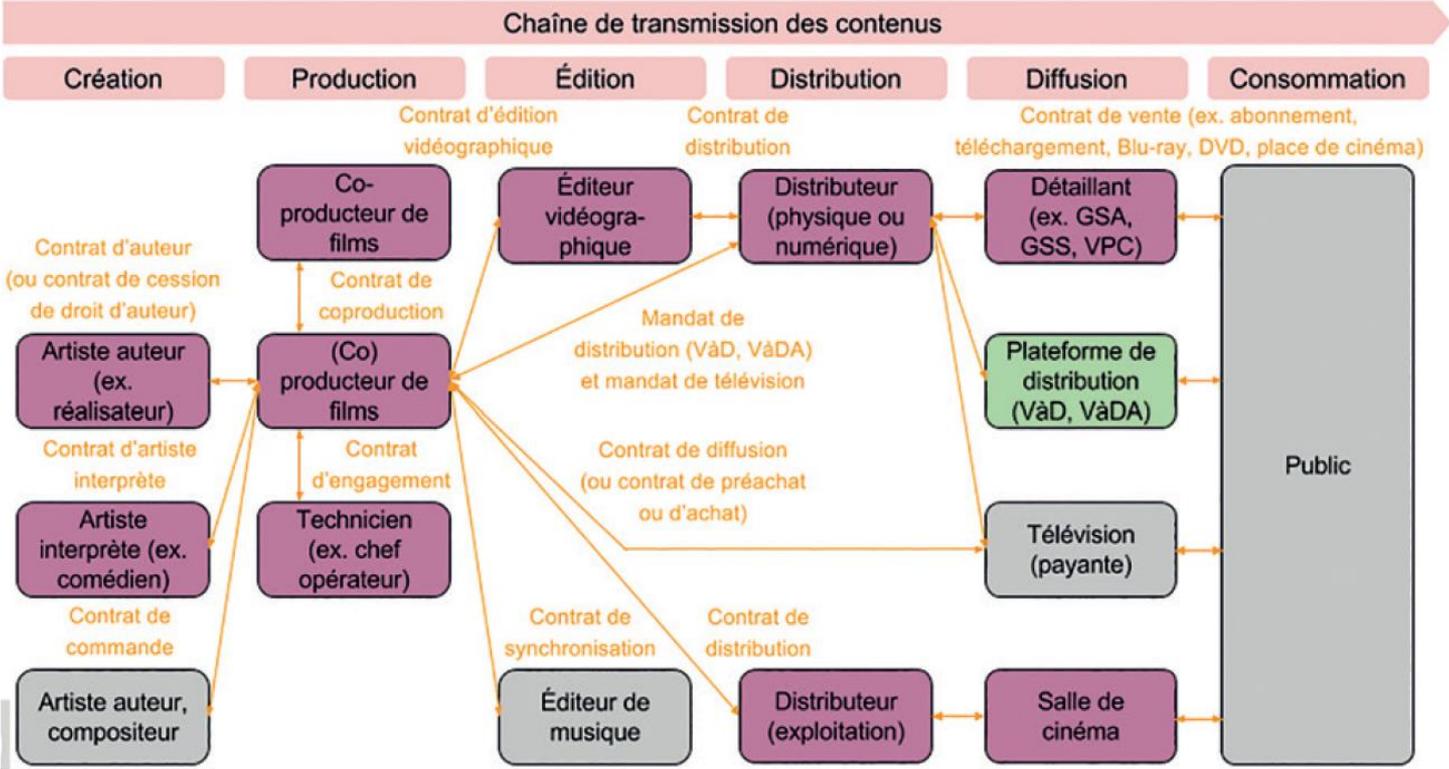
Possibilité de « côter » les titres non cotés

Exemple des dettes commerciales (délais de paiement)
Titre de dettes de courts termes entre entreprises
Part importante des financements d'entreprises
Le créancier peut avoir besoin d'utiliser immédiatement
Aujourd'hui, cession au cas par cas (affacturage), coûteux

Organiser un second marché des dettes comm.

Créer un blockchain entre entreprises
Y inscrire les transactions, délais, réalisations...
Possibilité de transférer les dettes de manière liquide
→ Quelle gouvernance ? Quel périmètre ?

Contrats dans le cinéma



Jérôme Pons (2017) *La mise en oeuvre de la blockchain et des smart contracts par les industries culturelles*, Annales des Mines - Réalités industrielles n° 2017/3, 81-90

Autres utilisations

Sociétés d'auteurs

UK (PRS for Music Limited) USA (Ascap), France (Sacem)
Blockchain privé pour relier les auteurs aux enregistrements
Peut être associés à des smart contract (notamment droits)

Registre des propriétés foncières

Géré de manière papier (puis informatisé) par les notaires
Principe de blockchain publique à mineurs privés (notaires)
Attachant caractéristiques PLU, valeur, servitudes, impôts...

Chaine d'approvisionnement

Marquage du produit, traçabilité, repackaging, contrefaçons
Blockchain privé, nœuds organismes chaine d'approvisionnement^t
Contrôle a posteriori car blocks indélébiles

Plan de la session

1. Qu'est-ce que la monnaie ?
2. Le blockchain et les cryptomonnaies
3. Smart contracts
- 4. Quelques perspectives sur l'AI***

Optimisation de protocoles

Le développement de l'informatique

- 1950 Test de Turing, pour mesurer l'intelligence d'une machine
- 1972 WABOT-1, robot humanoïde, conçu à l'Université Waseda (Japon)
- 1986 Algorithme d'apprentissage des réseaux de neurones

Communication grand public

- 1997 Deep Blue d'IBM bat Garry Kasparov, champion d'échecs
- 1999 Sony lance Aibo, un robot chien doté d'intelligence artificielle
- 2009 Google utilise voitures autonomes pour cartographier Street View
- 2011 IBM Watson bat des champions humains au jeu télévisé Jeopardy!
- 2016 AlphaGo bat Lee Sedol, le champion du monde de Go

Accélération

- 2020 OpenAI lance GPT-3, un modèle de traitement du langage
- 2021 DeepMind résoud le problème du repliement des protéines
- 2022 Google AI introduit des systèmes de dialogue avancés
- 2024 IA générative devient des outils commerciaux dans secteurs variés

Le problème de l'alignement

Mécanisme classique de management par objectif

Nœud central définit des indicateurs et objectifs

Les opérateurs adaptent leur comportement

→ pour optimiser les indicateurs

→ pas directement pour remplir les objectifs souhaités

Détournement, avec potentiellement effet contre-productif

Le problème de la perte de contrôle

Le problème d'alignement est encore plus important en IA

Développement de systèmes capables de s'auto-améliorer

Selon consignes/objectifs définis au démarrage du processus

Comment assurer la continuité de l'alignement ?

La crise chez OpenAI

Création comme association non lucrative en 2015

Co-présidents Sam Altman et Elon Musk

Investisseurs Peter Thiel, Amazon WS, des capital-risques

Budget initial de 1 Mds\$ non utilisés les premières années

But : créer IA générale sûre et bénéfique à toute l'humanité

Open source, indép. des monopoles et contraintes finance

Développement accéléré

2019 Structure lucrative pour attirer nouveaux investisseurs

Microsoft investit 1 Mds\$ (contre accès privilégié)

Fin de l'open access, préparation version commerciale

2022 Commercialisation ChatGPT, Microsoft investit 10 Mds\$

Levée de fonds 90 Mds\$, rachat des parts des employés

La crise chez OpenAI

Développement accéléré

- 2019 Structure lucrative pour attirer nouveaux investisseurs
Microsoft investit 1 Mds\$ (contre accès privilégié)
Fin de l'open access, préparation version commerciale
- 2022 Commercialisation ChatGPT, Microsoft investit 10 Mds\$
Levée de fonds 90 Mds\$, rachat des parts des employés

La crise au sein d'OpenAI

- Scission croissante entre accélérationnistes et catastrophistes
- Orientation croissante accélérationniste de l'entreprise
- 17/11/2023, CA d'OpenAI démet Sam Altman de poste PdG
- 22/11/2023, retour de Sam Altman en tant que PdG
- Modification du CA, avec entrée de Microsoft

Nouveaux Modèles économiques

Chapitre 2
La smart économie