Economie numérique / Blockchain et cryptomonnaies

@Patrick Duc, 2023

Concepts

- Bitcoin et cryptomonnaies
- Blockchain
- Attaque byzantine et consensus
- Types de consensus
- Blockchain et Decentralized Finance

Bitcoin

- Qu’est-ce que le Bitcoin et à quoi sert-il ?

Bitcoin et monnaie virtuelle

- Le Bitcoin désigne à la fois une cryptomonnaie (jeton = bitcoin) et le protocole associé (Bitcoin)
- Le protocole Bitcoin a été conçu pour permettre l'existence d'une **monnaie virtuelle** ou **cryptomonnaie**

Monnaie virtuelle

- Qu’est-ce qu’une monnaie virtuelle ?

Monnaie virtuelle

- Caractéristiques d'une monnaie virtuelle
  - Monnaie **digitale**
    - Pas de billets ou pièces
  - **Sans intervention** des banques ou états
    - Pas de cours légal (sauf exception), pas de contrôle des états
  - **Décentralisée**
    - Pas d'organisme central pour enregistrer et vérifier les transactions
  - Pas de valeur **intrinsèque**

Monnaie fiduciaire

- Caractéristiques d'une monnaie **fiduciaire**
  - Monnaie émise par **un état** (exemple : livre sterling £) ou **un groupe d'états** (exemples : euro €; dollar américain $)
  - Pas de **valeur intrinsèque** (pas adossée à l'or, par exemple)
  - Gestion **centralisée**
    - Banque centrale d'un état (Bank of England ou **BoE**; Bank of Japan ou **BoJ**)
    - Banque centrale d'un groupe d'états (pays européens utilisant l'euro : Banque centrale européenne ou **BCE**; Etats-Unis : Federal Reserve System ou **Fed**)

Monnaie virtuelle

- Où sont enregistrés les échanges de monnaie virtuelle ?

Monnaie virtuelle et blockchain

- Les échanges sont enregistrés dans une chaine de blocs ou **blockchain**

Blockchain

- Qu’est-ce qu’une blockchain, précisément ?

Blockchain

- Une blockchain est un **registre public**, **distribué** (*distributed ledger*) et **décentralisé** (*decentralized*)
  - un registre car elle contient l'enregistrement d'informations (transactions financières, délivrance de diplômes, données d'origine de marchandises, etc.)
  - public car tout le monde (en général) a accès en lecture à la blockchain
  - distribué car le registre est répliqué en de nombreuses instances
  - et décentralisé car sa gestion est réalisée par un ensemble large de participants d'importance égale

Blockchain

- Les enregistrements dans une blockchain représentent un historique et surtout une **référence**
- Par conséquent, ils ne doivent pas pouvoir être modifiés
  - la blockchain doit être protégée en **intégrité**

Rappels de cybersécurité

- Intégrité
  - Propriété d'une donnée dont **toute modification** est **détectable**
  - Technique pour assurer l'intégrité : le calcul d'une empreinte digitale ou condensat (*hash*) de la donnée
- Authenticité
  - Propriété d'une donnée dont on connait avec certitude **l'origine**
  - Technique classique pour assurer l'intégrité : la signature (numérique ou physique)

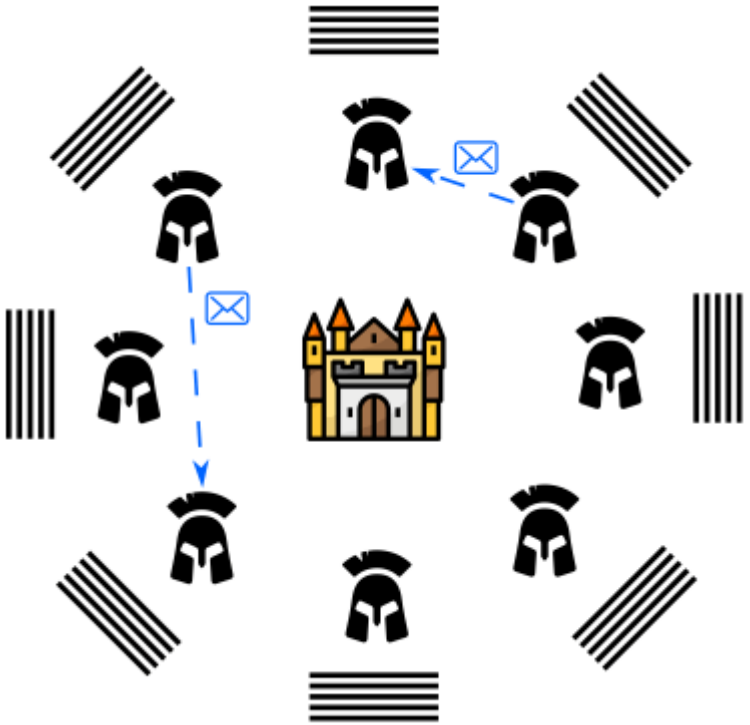
Rappels de cybersécurité

- Confidentialité
  - Propriété d'une donnée qui n'est **claire** que sous certaines conditions (en particulier la connaissance d'un **secret**)
  - Technique pour assurer la confidentialité : le chiffrement

Blockchain et attaque byzantine

- Les enregistrements dans une blockchain représentent la référence
  - la blockchain doit être protégée en **intégrité**
- Risque : un pirate dépense plusieurs fois la même somme (en effaçant les dépenses précédentes)
  - c'est le problème de la **double dépense**
  - ce genre d'attaque est appelée une **attaque byzantine** (par référence au problème des **généraux byzantins)**

Le problème des généraux byzantins



Préparation de l'attaque par échange de messages.

L'attaque doit avoir lieu à un moment précis, avec suffisamment de généraux.

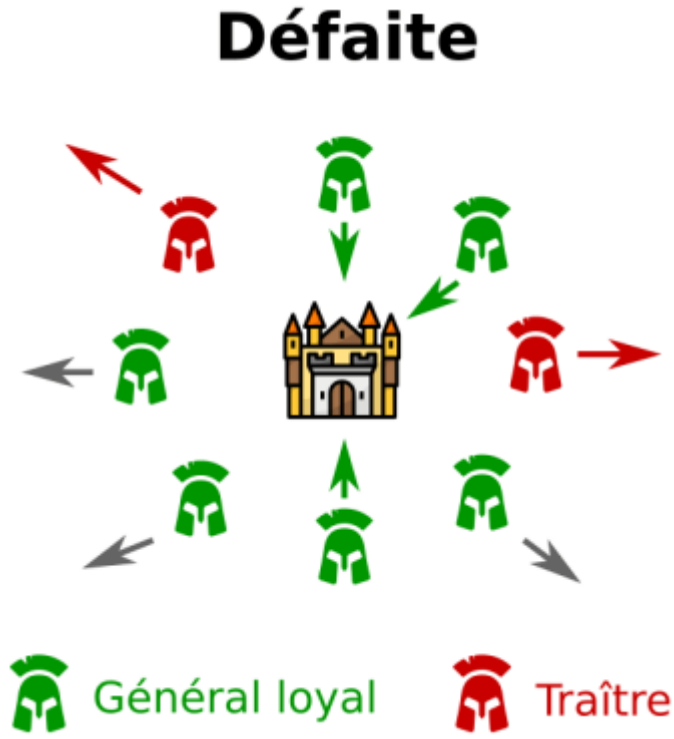
Le problème des généraux byzantins

@ viresinnumeris.com

Attaque coordonnée menant à la victoire.

L'heure de l'attaque a été passée à tous les généraux, ceux qui sont honnêtes ont suivi la consigne.

Le problème des généraux byzantins



@ viresinnumeris.com

Attaque non coordonnée menant à la défaite.

Des généraux traîtres ont envoyé des informations erronées à d'autres généraux (heure de l'attaque).

Le problème des généraux byzantins

- Quel système / protocole permet de s'assurer que les traîtres ne vont pas mener à une défaite ?
- Le point clé est que ce système est **décentralisé** : il n'y a **pas** d'**authorité centrale** pour organiser l'attaque
  - Les généraux sont tous égaux / ce sont des **peers**
- Si authorité centrale, l'attaque est bien organisée et fonctionnera… sauf si l'entité centrale est corrompue !

Blockchain et consensus

- Trouver une solution à ce problème peut se faire en définissant un **consensus**
- Un consensus est une organisation / un algorithme qui permet de décider si une information est **considérée** comme correcte ou pas
- Dans le cas d'une blockchain, un consensus permet de choisir les informations (transactions financières, par exemple) qui sont considérées comme **valides**

Preuve de travail / Proof of Work (PoW)

- Le consensus proposé par le protocole Bitcoin est basé sur une solution probabiliste : une **preuve de travail (proof of work** ou **PoW)**
- PoW = compétition entre noeuds du réseau (**mineurs**) pour résoudre le plus rapidement possible un challenge cryptographique
  - Le gagnant gagne un certain nombre de jetons Bitcoin
- Ce challenge cryptographique est **très compliqué** à résoudre
  - Il demande beaucoup de **travail** de calcul

Preuve de travail / Proof of Work (PoW)

- La solution du challenge consiste en une nouvelle entrée dans la blockchain (un **bloc**)
- Ce bloc contient une liste de transactions récentes qui sont temporairement considérées comme valides
- La vérification de la solution est très simple
  - Les noeuds qui effectuent cette vérification sont appelés des **validateurs**
  - Ils sont aussi rémunérés pour cela – mais beaucoup moins

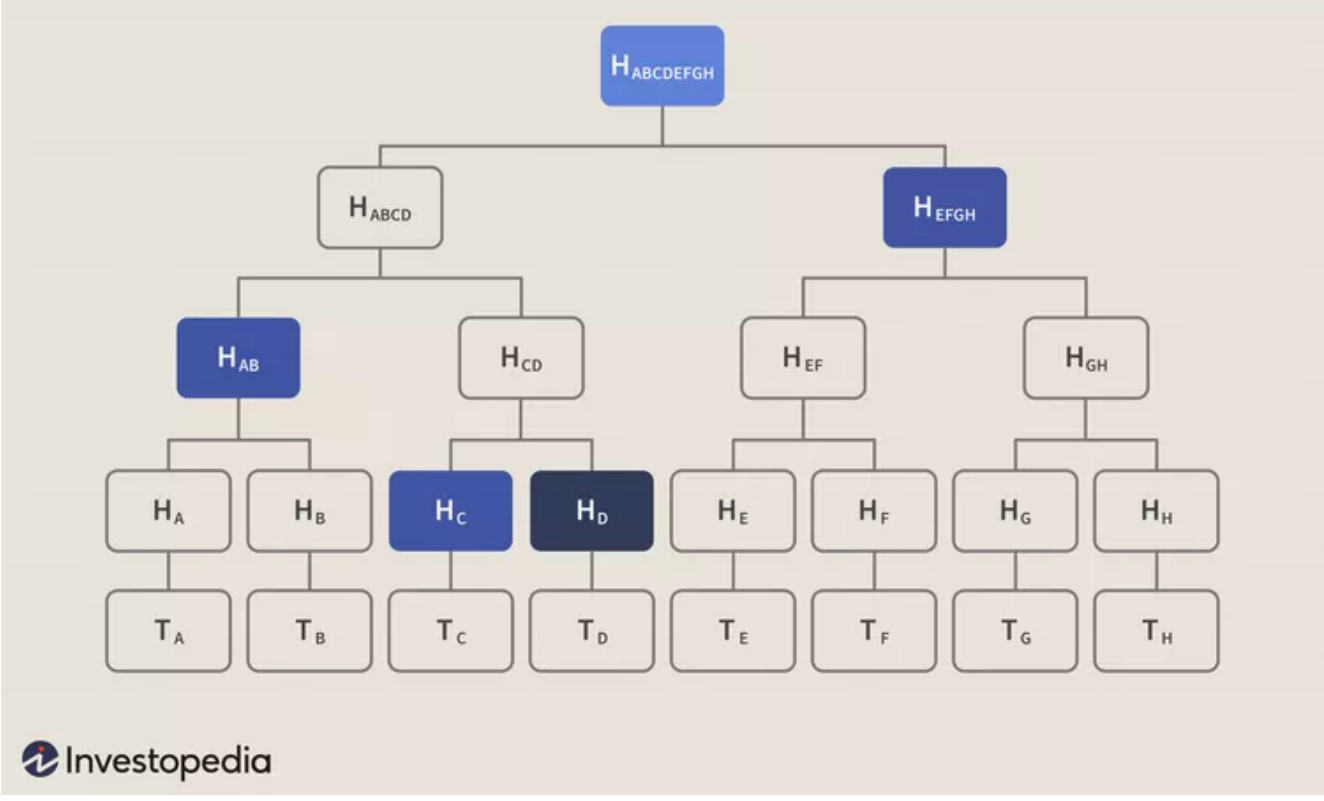
Preuve de travail et sécurité

- La sécurité apportée par la preuve de travail réside dans le fait qu'il est **extrêmement compliqué** de revenir en arrière
  - Par exemple pour effacer une transaction précédente et pouvoir ainsi effectuer une double dépense

Preuve de travail et sécurité

- Les blocs sont en effet chainés entre eux
  - Chaque entête de bloc inclut le hash de l'entête du bloc précédent
  - Chaque entête de bloc inclut la racine de l'**arbre de Merkle** des transactions qu'il contient
  - Modifier les transactions d'un bloc passé implique de regénérer un nouvel arbre de Merkel sans modifier le hash du bloc → **≈ impossible**

Preuve de travail et sécurité



Un arbre de Merkle (basique)

Preuve de travail : le minage

- Calcul du hash d'un nouveau bloc
  - Le hash est calculé sur l'entête du nouveau bloc (candidat pour l'ajout)
  - Cet entête contient 6 champs :
    - le numéro de version du protocole
    - le hash du bloc précédent dans la chaine
    - la racine de Merkle (*Merkle root*) des transactions incluses dans le bloc
    - l'heure de création du bloc
    - la valeur maximale autorisée du hash (*hash target*)
    - un champ libre (*nonce*)

Preuve de travail : le minage

- Calcul du hash d'un nouveau bloc
  - Le hash calculé doit être inférieur ou égal à la valeur indiquée par le champ hash target
    - Un certain nombre de 0 puis une valeur sur 3 octets
  - Le mineur modifie le champ *nonce* lors de chaque calcul afin de générer un hash différent à chaque fois
  - Si le hash calculé est inférieur ou égal à la valeur indiquée par le *hash target* (seuil de hash), alors le bloc est considéré **valide** et la valeur du nonce est appelée *golden nonce*

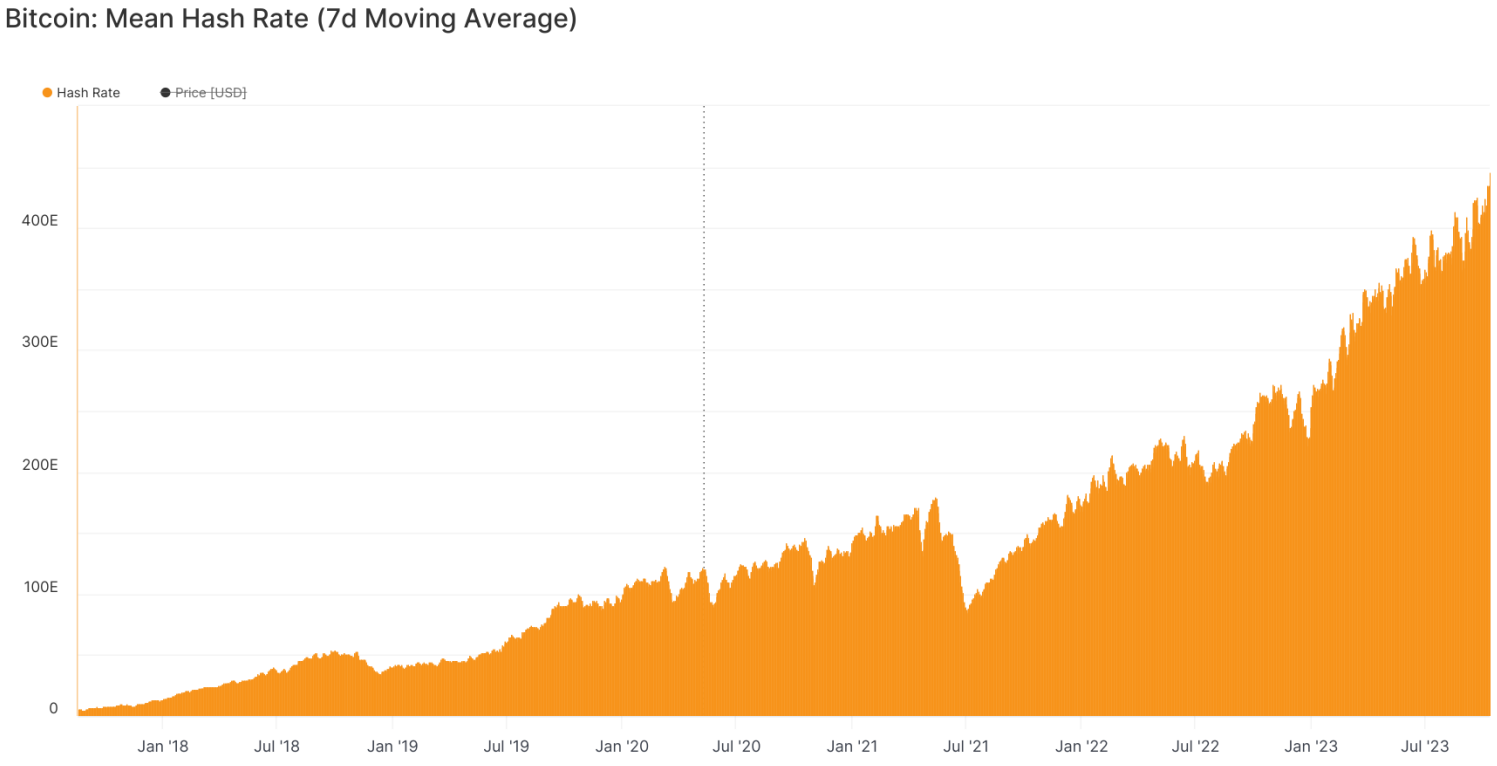
Preuve de travail : le minage

- Modifier un bloc d'une blockchain est difficile car :
  - il faut générer un bloc dont la nouvelle valeur de hash respecte le seuil de hash
  - et surtout il faut faire accepter le nouveau bloc par les autres validateurs !
- Cette dernière contrainte peut être contournée si on contrôle au moins 51% des validateurs
  - attaque "des 51 %" ou attaque Goldfinger

Preuve de travail : le minage

- Industrie du minage (*bitcoin mining farms*)
  - Gros sites industriels (fermes)
  - Processeurs adaptés (GPU)
  - Processeurs dédiés (ASIC)
  - Puissance de hashage (octobre 2023) : entre 400 et 500 exahashs par seconde
    - 450.10^{18} hashs par seconde
    - ...soit 450 000 000 000 000 000 000 hashs par seconde

Preuve de travail



glassnode

@Patrick Duc, 2023

Preuve de travail

- Quel est le gros inconvénient de la preuve de travail ?

Preuve de travail et écologie

- Le minage d'un bloc représente une **énorme** consommation d'électricité
  - Car il y a de très nombreux mineurs
    - Attirés par la prime offerte pour ajouter un bloc à la blockchain
  - Et ils utilisent de gros moyens
    - fermes de minage avec GPU et ASIC

Preuve de travail et écologie

- Les activités de minage représentaient en début 2022 0.55 % de la consommation électrique mondiale
  - Soit l'équivalent d'un pays à consommation moyenne (Suède, Malaisie)

- L'empreinte carbone du minage de bitcoins est massive
  - Equivalent à la production de CO2 de (au choix) l'Irlande, la Nouvelle-Zélande, la Hongrie ou le Pérou (chiffres de début 2022)

Preuve d'enjeu / Proof of Stake (PoS)

- Le consensus proposé par le protocole **Ethereum** est basé sur une solution différente : une **preuve d'enjeu (proof of stake** ou **PoS)**
- Un noeud du réseau Ethereum voulant pouvoir proposer le prochain bloc de transactions doit mettre **sous séquestre** ("staker") une certaine somme d'argent, son enjeu (*stake*)
- Le choix du gagnant sera fait de manière **aléatoire** mais en pondérant le hasard par l'enjeu des noeuds : la probabilité d'être choisi pour ajouter le bloc suivant sera **fonction de l'enjeu** de chaque noeud

Preuve d’enjeu

- Un validateur votant comme la majorité des autres noeuds reçoit aussi une récompense
- Un validateur dénonçant un noeud malhonnête reçoit aussi une récompense
- A l’inverse, un validateur “malhonnête“ ou peu réactif (trop lent) peut voir une partie de son dépôt supprimé (*slashing*)

Autres consensus

- Il y a de nombreux autres consensus
  - Proof of Capacity
    - **espace disque disponible** sur un disque et utilisable par la blockchain pour stocker des valeurs de hash possibles
    - les participants reçoivent des jetons en fonction de l'espace disque proposé
    - Exemple de cryptomonnaie : Chia, SigNum
  - Proof of Authority
    - seuls **certains noeuds** peuvent valider les transactions et créer de nouveaux blocs; utilisés dans des blockchains privées (entreprises ou groupes d'entreprises)

Autres consensus

- Autres consensus
  - Proof of Burn
    - il faut prouver que l'on a **consommé des jetons** pour avoir le droit de proposer un nouveau bloc
    - Exemple de cryptomonnaie : SlimCoin
  - Proof of Elapsed Time
    - proposé par INTEL; ressemble à une simple **loterie**
  - Proof of Identity
    - Requiert de prouver son **identité** (via un moyen officiel, des données biométriques, un compte de réseau social, ...)

Blockchain et DeFi

- Décentralisation des protocoles blockchain ==> création d'un **nouveau paradigme** pour l'économie financière
  - Emancipation d'une autorité centrale
  - "*Decentralised finance (**DeFi**) builds on distributed ledger technologies (DLT) to offer services such as trading, lending and investing without using a traditional centralised intermediary*"

    (Banque des Règlements Internationaux / The Technology of Decentralized Finance)

Blockchain et DeFi

- Plus besoin d'une autorité financière centrale
  - France : AMF = Autorité des Marchés Financiers
  - Etats-Unis : SEC = Securities Exchange Commission
- Plus besoin d'intermédiaires financiers (banques, courtiers)
- Les échanges (prêts, trades) se font en peer-to-peer (P2P)

Blockchain et DeFi

- Avantages
  - Plus rapide
  - Moins cher
  - Disponible partout dans le monde
  - Permet à un particulier de générer des revenus

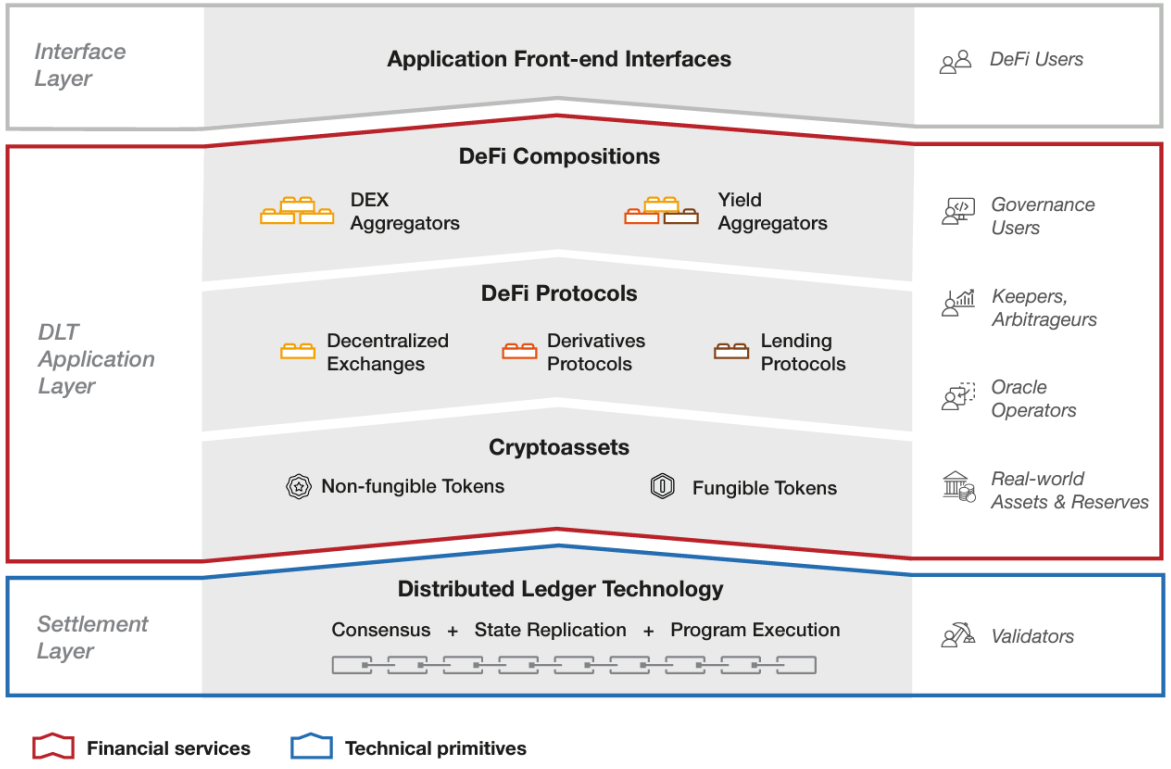
Blockchain et DeFi

- Inconvénients
  - Mécanismes complexes
  - Très dépendant de la technologie
  - Volatilité élevée
  - Risque de fraudes
    - Comment les gérer ? Quel organisme en est responsable ?

Blockchain et DeFi

- La DeFi est implementée au travers de **smart contracts**
- Un smart contract est un programme informatique qui
  - fournit une fonctionnalité financière / représente une application financière
  - et s'exécute sur une blockchain adaptée (genre Ethereum)
- Services financiers proposés
  - emprunts (*lending*)
  - bourses d'échange décentralisées (*DEX*)
  - produits dérivés

Modèle de référence de la DeFi



Modèle à 3 couches :

* fondation (*settlement*)
* application (*application*)
* IHM (*user interface*)

@ Banque des règlements Internationaux, 2023

Et la FinTech ?

- FinTech = Financial Technology
- Nouvelles technologies pour fournir et utiliser des services financiers
  - Gestion d'investissements (High Frequency Trading par exemple)
  - Gestion de compte de particulier
  - Levée d'argent (crowdfunding)
  - …

DeFi vs. FinTech

	Financial technology (FinTech)	Decentralized finance (DeFi)
What's at the core:	Any technology	Blockchain-based solutions
What it does:	Improve traditional financial services	Provide cryptocurrency-based financial services
Management:	Centralized	Decentralized
Who's in charge:	Financial institutions	Regular users

www.apriorit.com

Bibliographie

- “Au-delà du Bitcoin“ / Jean-Paul Delahaye / Editions Dunod, 2022
  - Présentation générale du monde de la blockchain et des cryptomonnaies

- https://www.bis.org/publ/work1066.pdf
  - Description de la DeFi et analyse de ses caractéristiques

FIN