

# La finance décentralisée

Alexis Direr

27 juin 2023

# Plan de la leçon

## Introduction

- La finance décentralisée

- Bénéfices de la Defi

- Une finance basée sur des smart contracts

## Bourses décentralisées

## Prêter/emprunter

- Facteur de santé

- Taux d'intérêt

## Gouvernance

- Les DAO

## Une Defi décentralisée ?

## La finance décentralisée

La finance décentralisée (DeFi) est un écosystème financier basé sur la blockchain et les smart contracts qui :

- permet aux utilisateurs de réaliser des transactions financières sans avoir besoin d'intermédiaires tels que les banques ou les gouvernements
- offre une alternative aux systèmes financiers traditionnels, en permettant aux utilisateurs de gérer leurs propres actifs et d'accéder à des services financiers sans permission

## Différences avec la finance traditionnelle

Fonction	Decentralized finance (Defi)	Centralized finance (Cefi)	Traditional finance (Tradfi)
Actifs	cryptoactifs	cryptoactifs	actions, obligations
Monnaie	stablecoins (DAI, LUSD)	stablecoins (USDC, USDT)	fiat (USD, EUR)
Paiement	MakerDao, Liquity	Circle, Theter	Visa, Mastercard
Échanges	Uniswap, Curve	Coinbase, Binance	Bourses
Dérivés	Synthetix, GMX	Binance, Deribit	CME, Eurex
Prêts	Aave, Compound		Courtiers

Un modèle bancaire et financier reposant sur des intermédiaires et leur bonne santé malgré des risques :

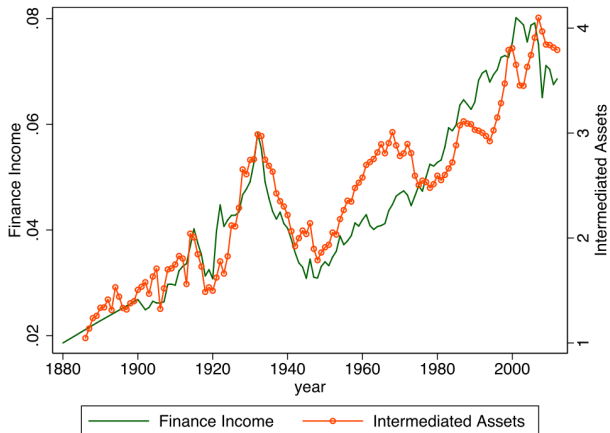
- banques fractionnaires (liquidités < dépôts)
- crédits sous-collatéralisés (les garanties apportées par les emprunteurs sont inférieures aux montants empruntés)

avec des gardes-fous :

- cadre juridique protecteur des épargnants et investisseurs (accords de Bâle, MIFID, ...)
- assurance des dépôts
- sélection stricte des emprunteurs
- conseillers financiers professionnels et certifiés

## Coûts de la finance traditionnelle (US)

Figure 2: Finance Income and Intermediated Assets over GDP



source



## Finance décentralisée, un système financier faiblement intermédiée

▷ absence de

- dépositaires (conservation des titres),
- chambres de compensation,
- courtiers,
- gérants de fonds, ...

= fonctions assumées par des smart contracts.

Illustration : processus de règlement d'une transaction financière en finance traditionnelle

1. Passation d'ordre : L'investisseur passe un ordre d'achat ou de vente d'un actif financier auprès de son intermédiaire financier (courtier, banque, etc.).
2. Exécution de l'ordre : L'intermédiaire financier transmet l'ordre à la bourse où l'actif est coté, laquelle met en correspondance les ordres d'achat et de vente en fonction des prix et des quantités. Une fois qu'un ordre d'achat correspond à un ordre de vente, la transaction est exécutée.
3. Compensation : La chambre de compensation de la bourse vérifie les détails de la transaction, et s'assure que les deux parties sont en mesure de respecter leurs obligations.

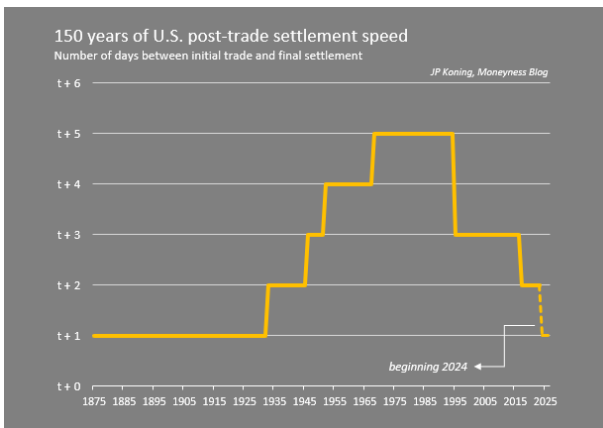


4. Règlement : les actifs financiers et les fonds sont échangés entre les parties par un transfert électronique des actifs financiers et des fonds entre les comptes des parties, généralement via un système de règlement centralisé, tel qu'un dépositaire central de titres (CSD).

5. Confirmation et reporting : Une fois la transaction réglée, les parties reçoivent une confirmation du règlement, qui inclut les détails de la transaction.

Le délai de règlement est généralement de deux jours ouvrables après l'exécution de la transaction.

## Délais de règlement au cours du temps



source

## Règlement d'une transaction financière en finance décentralisée :

1. Passation de l'ordre : l'investisseur connecte son wallet à l'échange (par exemple Uniswap) et remplit les détails de la transaction (actifs échangés, quantités, limite vs. au marché, frais de gas).
2. Exécution de l'ordre : le wallet propage la transaction au sein du réseau de validateur jusqu'à son exécution.
4. Règlement : les actifs financiers et les fonds sont échangés entre les parties par une mise à jour de l'état des smart contracts.
5. Confirmation et reporting : L'investisseur reçoit une confirmation du règlement, vérifiables via l'explorateur de la blockchain.

Le délai de règlement est fonction des frais de gas payé et va de quelques secondes à quelques minutes la plupart du temps.

## Intérêts de la finance décentralisée

- ▷ Accessible (toute personne disposant d'une connexion internet)

Les services financiers traditionnels sont souvent limités par des barrières géographiques, des exigences de crédit et des frais élevés.

- ▷ Auto-conservation des fonds (wallets avec clés privées)

- ▷ Sans permission

N'importe qui peut déployer un contrat sur une blockchain, interagir avec, ...



## ▷ Transparence

Les transactions et les contrats sont vérifiables sur la blockchain, ce qui permet aux utilisateurs de :

- vérifier les transactions
- vérifier le code
- comprendre les mécanismes de fonctionnement des services financiers décentralisés



## ▷ Immuabilité

Une fois qu'une transaction est enregistrée sur une blockchain, elle ne peut pas être modifiée, ce qui garantit que la transaction est irréversible et que les enregistrements sont infalsifiables.

→ les ruptures ou renégociations de contrat ne sont pas possibles (*code is law*)

→ les recours au système juridique sont limités aux situations de hacks et comportements frauduleux

▷ Résistance à la censure

Personne ne peut interdire ou fermer une application décentralisée.



hayden.eth



@haydenzadams



It's an immutable smart contract on Ethereum. I have no ability to turn it off

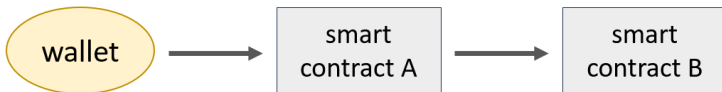
If you're talking about frontends there are ~50 independent ones

Plenty of volume is on-chain and doesn't go through any frontend

I could try tweeting "can everyone please stop trading" though

source

▷ Composabilité (interopérabilité) : les applications DeFi peuvent être combinées et interagir entre elles.





## Valeur totale verrouillée (*total value locked, TVL*) dans les smart contracts sur Ethereum



observé le 17/04/2023

Source



## Quelques applications et protocoles DeFi :

- prêts/emprunts (Aave, Compound, ...)
- échanges décentralisés (Uniswap, dydx, ...)
- produits dérivés (Ribbon, Dopex, ...)
- gestion d'actifs (Yearn, Set Protocol)
- stablecoins décentralisés (LUSD, DAI, ...)

## Une finance basée sur des smart contracts

Smart contracts : programmes informatiques courts (**scripts**) autonomes qui vivent sur les blockchains, et sont exécutés lorsque des conditions prédéterminées sont remplies.

Les smart contract permettent de réaliser des transactions et des accords fiables entre des parties disparates et anonymes, sans qu'il soit nécessaire de recourir à une autorité centrale, à un système juridique ou à un mécanisme d'exécution externe.

Deux types de comptes :

- les comptes externes (*externally owned account*, EOA)
- les comptes de contrat (*contract account*, CA)

Les utilisateurs peuvent envoyer une transaction d'un EOA à un autre EOA, ou d'un EOA à un CA. Les deux types de compte peuvent détenir des cryptoactifs.

Un smart contract est une collection de fonctions (méthodes).

Lorsqu'une transaction "réveille" un smart contract et que les critères d'exécution d'une de ses fonctions (méthodes) sont remplis, le code associée à la fonction est exécuté.



## Les smart contracts : des dépositaires et distributeurs de jetons



référence

## Exemples de protocoles de finance décentralisée

Une bourse décentralisée : Unisocks

Un protocole de prêt et emprunts de cryptoactifs : Aave

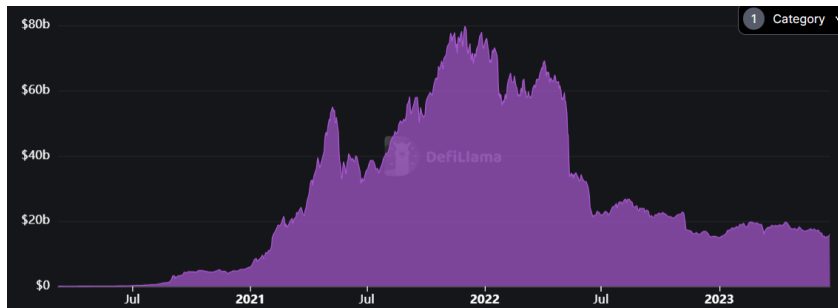
## Bourse décentralisée

Une bourse décentralisée (*decentralized exchange*, DEX) permet l'échange de cryptoactifs sans nécessité d'un intermédiaire.

La plupart des DEX suivent le modèle des teneurs de marché automatisés (*automated market maker*, AMM), inventé par Uniswap en novembre 2018.

Principe d'un AMM : détermination algorithmique du prix d'échange

Valeur totale (total value locked, TVL) dans les DEX ( $\approx 20$  b\$)

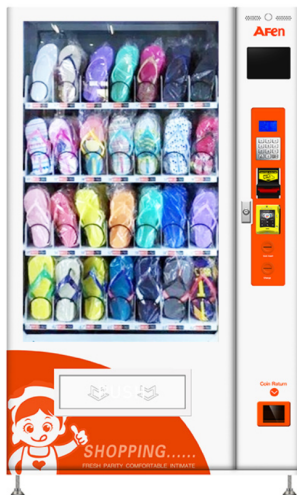


sources : 1





# Une bourse décentralisée : un distributeur de paires de chaussettes



## Fonctionnement d'Unisocks

\$\$SOCKS est un jeton qui donne droit à une véritable paire de chaussettes en édition limitée, expédiée n'importe où dans le monde.

Le jeton peut être revendu à tout moment sur une bourse décentralisée.

Un pool de jetons a été créé à l'origine avec 500 jetons SOCKS et 35 ETH pour un prix de départ de  $35/500 = 0,07$  ETH =  $0,07 \times 170$  USD (mai 2019) = 12 USD.

source : [1](#), [1](#)

## Logique du smart contract :

- jeton du protocole : SOCKS
- échange SOCKS  $\rightarrow$  ETH : prix SOCKS  $\nearrow$
- échange ETH  $\rightarrow$  SOCKS : prix SOCKS  $\searrow$

$\rightarrow$  chaque achat/vente fait varier le prix des jetons jusqu'à trouver un équilibre, fonction de la demande et de l'offre de paires.

## Hors smart contract :

- 1 SOCKS brûlé = 1 paire de chaussettes reçue par la poste

source : 1

## unisocks token (SOCKS)

**\$68.15 USD**

dynamically priced socks



purchasing a **SOCKS** entitles you to 1 *real* pair of limited edition socks, shipped anywhere in the world.

Buy SOCKS

Sell SOCKS

250/500 available

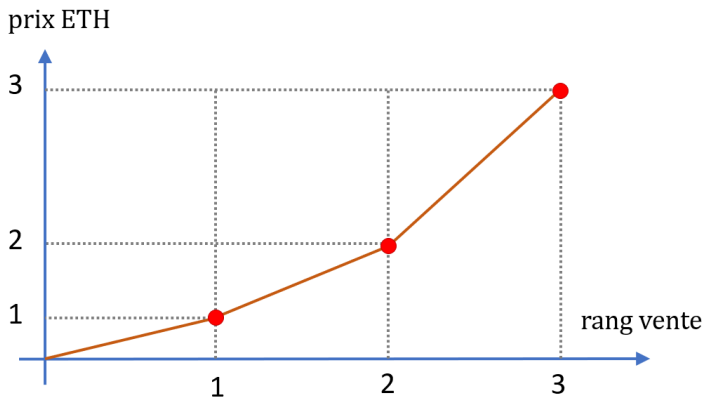
Redeem Coming Soon!™

## Une courbe algorithmique de prix

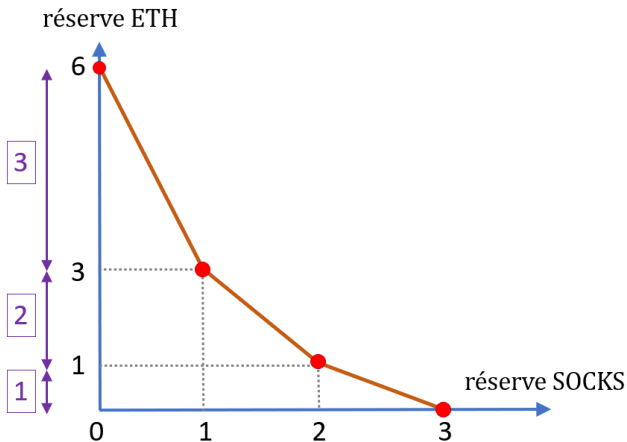


source : 1

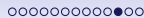
## Une courbe de prix simplifiée (3 paires)



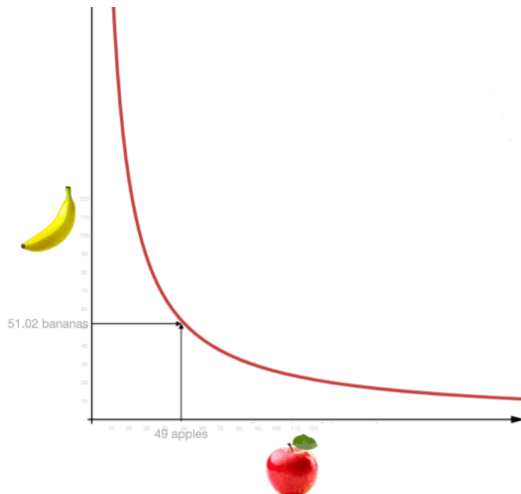
## Relation entre les réserves de paires et d'ETH (avec 3 paires)



vu le 23/06/2023 source : 1



## Fractionnement des jetons : courbe continue



source : 1



Fractionalisation de la propriété

Pool Uniswap SOCKS/ETH

Faire un échange : SOCKS/ETH

## Prix SOCKS/ETH



vu le 23/06/2023

prix min : 0,38 ETH (41\$), max : 102 ETH (200 000\$)

source : [1](#)

## Prêter et emprunter

L'exemple d'Aave : protocole décentralisé pair à pair de prêt et d'emprunt de cryptoactifs

Créé en 2017 (ETHLend), financé via une ICO (*Initial Coin Offering*) de 16.5 millions de dollars.

5,6 b\$ de valeur bloquée (TVL) dans le protocole (3ème protocoles en termes de TVL)

vu le 24/06/2023

sources : [1](#), [2](#), [3](#)

## Fonctionnement

Des utilisateurs déposent des actifs dans des smart contracts dédiés. D'autres utilisateurs peuvent emprunter ces actifs contre le paiement d'un intérêt.

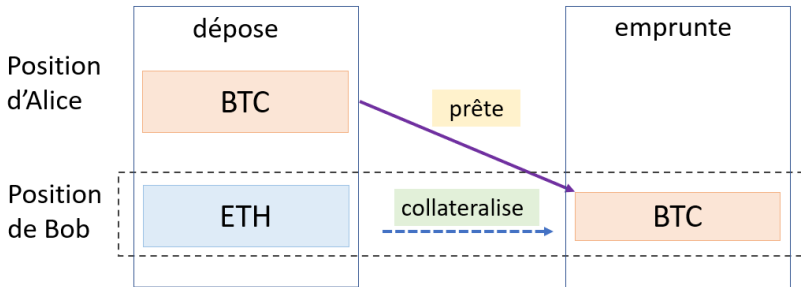
Pour emprunter, les utilisateurs doivent également déposer des actifs au titre de garantie (collatéral) sur la plateforme.

La valeur de cette garantie doit être supérieure à la valeur du montant emprunté, afin d'assurer la solvabilité de l'emprunteur et de protéger les prêteurs contre les risques de défaut de paiement.

Pas d'échéance de remboursement.

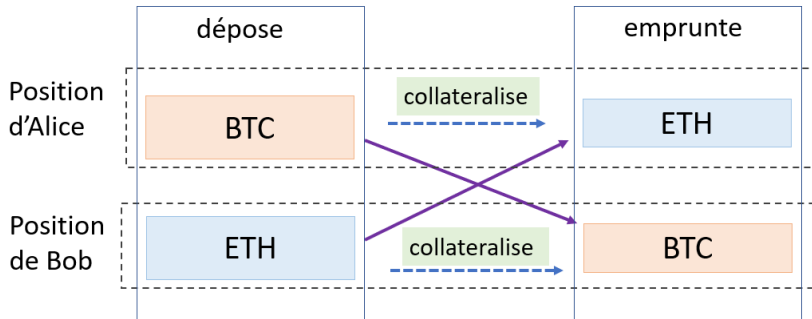
Sans permission : n'importe qui peut déposer et emprunter des actifs.

Schéma simplifié avec deux actifs et une position d'emprunt  
Alice prête indirectement à Bob :



Les ETH de Bob sont bloqués tant qu'il n'a pas remboursé les BTC.

Deux actifs et deux positions d'emprunt croisées.



Marchés Aave : 1

Quand liquider la position d'un emprunteur ?

Seuil de liquidation : ratio prêt/valeur (LTV) : montant maximum d'actifs qui peut être emprunté pour une valeur de collatéral donnée :

$$\text{Loan to Value (LTV)} = \max \frac{\text{valeur de l'emprunt}}{\text{valeur du collatéral}}$$

Exemple : LTV de ETH = 80 %

→ je peux emprunter des ETH jusqu'à 80 % de mon collatéral

→ seuil de liquidation = 0.8 si la valeur de mon collatéral baisse (ou le prix des ETH augmente).

Comment mesurer la solvabilité d'un emprunteur ?

Facteur de santé (*health factor*) : ratio de la valeur du collatéral déposé par l'utilisateur par la valeur de l'emprunt en cours :

$$HF = \frac{\text{valeur du collateral} \times \text{seuil de liquidation}}{\text{valeur de l'emprunt}}$$

Plus le facteur de santé est élevé, plus la position de l'emprunteur est considérée comme sûre. Un facteur de santé :

> 1 : l'emprunteur est solvable

< 1 : l'emprunteur est sous-collatéralisé ; sa position est à risque de liquidation.



## Exemple

Alice dépose 1 ETH dont le prix de marché est actuellement \$2000.

Elle souhaite emprunter des BTC dont le prix de marché est \$30000.

BTC maximum empruntable :

$LTV(ETH) \times 2000 = 0,8 \times 2000 = \$1600$  de BTC

soit  $1600/30000 = 0,053$  BTC

Si Alice empruntait 0,053 BTC, son HF serait de 1.

Alice est prudente et décide d'emprunter 0,04 BTC.

$$\rightarrow HF = (0,8 \times 1 \times 2000) / (0,04 \times 30000) = 1,33.$$

Si le prix de l'ETH baisse et/ou le prix du BTC augmente, son HF se rapproche de 1.

A prix du BTC donné, si le prix de l'ETH descend en dessous de  $p$  avec

$$\frac{0,8 \times 1 \times p}{0,04 \times 30000} = 1$$

soit :

$$p = \frac{0,04 \times 30000}{0,8} = 1500$$

La position d'Alice est liquidable.



## Liquidation

Si un emprunteur devient sous-collatéralisé ( $HF < 1$ ), sa position est liquidable.

Interviennent une troisième catégories d'agents : les liquidateurs.

→ remboursent tout ou partie de l'emprunt à la place de l'emprunteur

→ saisissent tout ou partie du collatéral de l'emprunteur

→ le vendent au prix de marché contre l'actif emprunté

→ conservent une fraction des actifs liquidés au titre de leur rémunération (bonus de liquidation)

La liquidation est sans permission

▷ n'importe qui peut exécuter la méthode `liquidationCall()` qui est un script de liquidation programmé dans le smart contrat `LendingPool` ([source](#)).

La liquidation garantit que les emprunts sont toujours remboursés.

→ protège le protocole contre les [mauvaises dettes](#) (valeur de la dette > garanties)



Exemple : le prix de l'ETH baisse et passe à  $\$1400 < \$1500$  : la position d'Alice est liquidée.

Le liquidateur commence par rembourser la dette d'Alice en BTC, soit 0,04 BTC, et se saisit d'une partie de la garantie, par ex. 0,94 ETH.

Il vend la garantie au marché contre des BTC et obtient :  
 $0,94 \times 1400 / 30000 = 0,043$  BTC.

Bonus de liquidation :  $0,043 - 0,04 = 0,003$  BTC, soit  
 $0,003 \times 30000 = \$120$ .

La dette d'Alice est effacée. Elle récupère 0,06 ETH et conserve les 0,04 BTC.

La santé du protocole dépend de la réactivité avec laquelle les positions à risque sont liquidées.

Si le prix chute trop rapidement, les positions peuvent être liquidés après que la valeur de l'emprunt ait dépassé celle de la garantie.

Exemple : le prix passe en dessous de \$1200 avant que les liquidateurs interviennent. La position d'Alice est partiellement liquidée : la totalité du collatéral est saisie et revendu mais le produit de la vente ne permet pas de couvrir 100 % de la dette.

Les taux d'intérêt pour les prêteurs et les emprunteurs sont déterminés par un mécanisme de marché basé sur l'offre et la demande.

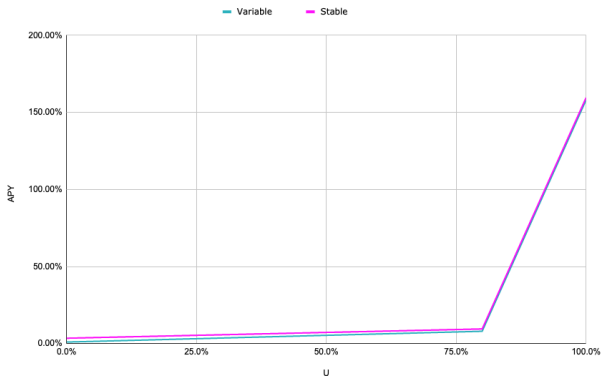
Les taux d'intérêt sont ajustés en temps réel en fonction de l'utilisation des fonds.

- Plus les fonds déposés sont utilisés pour emprunt, plus le taux d'intérêt est élevé ;

→ incite les prêteurs à déposer davantage de fonds et les emprunteurs à rembourser leurs prêts.

- Moins les fonds sont utilisés, plus le taux d'intérêt est bas.

## Courbe du taux d'intérêt : Exemple du DAI



U : taux d'utilisation (U=60 % signifie que 60 % des dépôts en DAI sont empruntés)

sources : 1, 2



## Gouvernance décentralisée

De la même manière que les entreprises ont besoin d'être gouvernées (avec une équipe de direction, des processus de décision hiérarchique, des circuits d'information, ...) de même un protocole de finance décentralisée a besoin de prendre régulièrement des décisions concernant son développement et stratégie

Différence majeure : un protocole Defi n'est pas décentralisé si la gouvernance est elle-même centralisée.

▷ Comment concevoir la gouvernance d'une organisation décentralisée ?

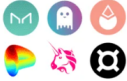

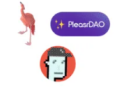

## *Decentralized autonomous Organizations (DAO)*

Détenues et gérées collectivement par leurs membres, les DAO sont des organisations natives du secteur des crypto-actifs.

- ▷ Organisation : communautés à l'échelle d'internet contribuant à des causes diverses
- ▷ décentralisées : sans faire confiance à un leader bienveillant ou une hiérarchie pour gérer les fonds ou les opérations.
- ▷ autonomes : des règles formalisées par des smart contracts définissent le fonctionnement de l'organisation et la manière dont les fonds sont dépensés.

Références : [1](#)

## Exemples de communautés régies par des DAO

Catégorie	Fonctions	Exemples
Gouvernance d'un protocole DeFi	Ces DAOs permettent aux gens de contribuer à un protocole DeFi en votant sur les modifications du protocole	
Média	Ces DAOs permettent aux gens de contribuer à un protocole DeFi en votant sur les modifications du protocole	
Collections	Ces DAO sont utilisées pour fédérer les communautés NFT/metaverse afin de soutenir le financement de projets artistiques	
Financement	Ces DAOs permettent le financement de projets web3	

## Les jetons de gouvernance

Une DAO est généralement gérée par ses membres grâce à l'utilisation de jetons de gouvernance (JG) qui offrent des droits sur la gouvernance du protocole

Le processus de décision est généralement scindé en deux phases :

- 1) les détenteurs de JG proposent des modifications via un processus de soumission de proposition
- 2) si certains critères sont remplis, la proposition est soumise à un vote selon la règle 1 JG = 1 voix.

Agrégateurs de propositions : Tally, Boardroom

## Exemple 1 : Curve Finance (decentralized exchange)

Pour contribuer à la gouvernance, les participants bloquent leur CRV dans un **locker** qui les verrouille et leur délivre des pouvoirs de vote veCRV proportionnels aux CRV déposés et à la durée de verrouillage :

- 4 ans : 1 CRV = 1 veCRV
- 1 an : 1 CRV = 0,25 veCRV
- 6 mois : 1 CRV = 0,13 veCRV
- 3 mois : 1 CRV = 0,06 veCRV

Les propositions sont débattues avant un éventuel vote sur le **forum** de gouvernance.

Pour mettre une proposition au vote, une personne doit détenir au moins 2500 veCRV (l'équivalent de 10000 **CRV** bloqués pendant un an) (environ \$10 000 au 23/04/2023)

Les votes se passent *on-chain* sur une **page dédiée** durant une fenêtre de temps d'une semaine.

La proposition, si elle est votée, est implémentée *off-chain*.

**source**

## Page de vote sur Curve.fi/dao

Vote info	Status
Ownership (51% / 50%) <b>Vote #27</b>	/ Open
<b>Description:</b>	59M:27S
Is Charlie asking for Ethereum on Telegram?	28/07/2020 22:08:13
<b>Proposed by:</b> 0x6ab6...9293a3	28/07/2020 23:08:13
<b>Votes:</b>	<b>Support</b>
<b>Yes:</b> 0% 0.00	0% (> 51% required)
<b>No:</b> 0% 0.00	<b>Minimum approval</b>
Voting with 2670.81 veCRV, you had 2670.81 veCRV at vote creation on snapshot block 6921232	0% (> 50% required)
<input type="button" value="Yes"/> <input type="button" value="No"/>	

## Exemple 2 : Aave

Les propositions sont débattues avant un éventuel vote sur le **forum** de gouvernance.

Les propositions doivent ensuite passer deux barrières :

- 1) Un vote de *temperature check* sur **Snapchat** (sans frais de gas)
- 2) Un second vote *on-chain* sur une **page dédiée** (avec frais de gas)

Les propositions sont formulées directement sous la forme de code exécutable : une transaction (un script) qui va interagir les smart contracts d'Aave.

Sources : [1](#), [2](#)



## Système de délégation

Les détenteurs des jetons **Aave** peuvent déléguer leur pouvoir de vote auprès de **délegués** dont le rôle est de :

- voter pour ou contre les *Aave Improvement Proposals* (AIP)
- proposer des AIP

Les délégations se font *on-chain* accessibles à partir d'UI comme **sybil.org**.

Des DAO (ex **Llama**) ou des associations d'étudiants (ex **Blockchain at Columbia**) sont spécialisées dans la gouvernance de DAO.

Source

# La Defi est-elle vraiment décentralisée ?

## Débats récents sur les DINO (*decentralized in name only*)

Avril 2023

### Finance « décentralisée » ou « désintermédiée » : quelle réponse réglementaire ?

Document de réflexion

AUTEURS

Olivier Fliche, Julien Uri, Mathieu Vileyn  
Pôle Fintech-Innovation



Pour évaluer le degré de décentralisation d'un protocole DeFi, plusieurs critères :

1. Infrastructure technique (manière dont les données et les transactions sont stockées et traitées)

Le protocole opère sur une blockchain publique et décentralisée, telle qu'Ethereum, où les données sont stockées et sécurisées par un grand nombre de nœuds répartis dans le monde entier.

2. Contrôle et gouvernance : le pouvoir de décision est réparti entre un grand nombre de personnes.

2bis. Distribution des tokens : si la gouvernance est fondée sur 1 token = 1 voix, la distribution des tokens n'est pas concentrée entre quelques mains.

3. Développement et maintenance du code : le code source du protocole est open source et accessible au public.

Permet à quiconque de vérifier, auditer et contribuer au développement du protocole, ce qui renforce la décentralisation et la transparence.

4. Risque de censure et d'interruption : aucune entité n'est en mesure de bloquer ou restreindre l'accès aux services financiers offerts par la plateforme.

4bis. Immuabilité des smart contracts : les smart contracts du protocole ne peuvent pas être l'objet de mises à jour majeures. Le cas échéant, les mises à jour doivent faire l'objet d'un vote contraignant des participants à la gouvernance.

## Une exception à l'immutabilité : les smart contracts évolutifs (*upgradeable*)

Architecture *Proxy Pattern* : modèle dans lequel un contrat proxy existe entre le contrat principal, qui contient la logique, et l'utilisateur. L'utilisateur accède au contrat Proxy, lequel transmet la transaction au contrat principal.

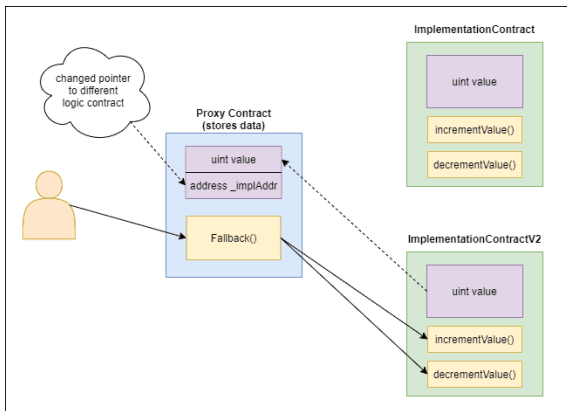
→ rend les contrats évolutifs

▷ Intérêt : permet la corrections de bugs et l'ajouts de fonctionnalités.

▷ Inconvénient : risque de centralisation du pouvoir et moindre résistance à la censure

source

## Fonctionnement des *Proxy Pattern*



source



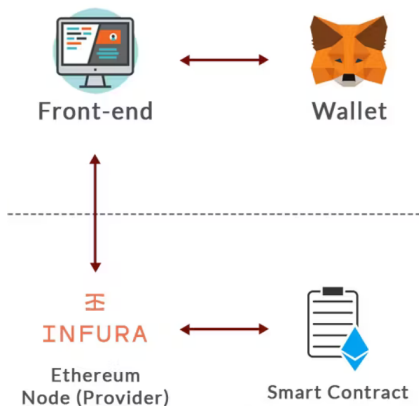
## Les interfaces utilisateurs

L'interface utilisateur (UI, front-end) d'une application englobe tous les éléments visuels et interactifs (menus, boutons, formulaires, listes déroulantes, notifications, ...) qui permettent à un utilisateur d'effectuer des actions, de recevoir des informations et de visualiser le résultat de ses interactions.

Les UI sont nécessaires pour intermédiaire la relation entre le smart contract et l'utilisateur.

Point de centralité ?

## Les interfaces utilisateurs web3



Les interactions avec les smart contracts étant sans permission, n'importe qui peut créer une UI qui se branche sur les smart contracts.

Exemples d'UI décentralisées :

- Différentes UI créée et maintenu sans permission par différents opérateurs (exemple : [Liquity](#))
- UI hébergés sur le réseau IPFS (exemple : [uniswap.eth.link/](https://uniswap.eth.link/))
- UI décentralisés versatiles : [etherscan](#), [abi.ninja](#)
- Applications qui se branchent sur des smart contracts et apportent des service supplémentaires (ex : [defisaver](#), [1inch](#), ...)

Par exemple, l'UI officiel d'Uniswap est complétée par plus de 50 UI gérées par des entités indépendantes.

## La gouvernance basée sur les jetons

Système de prise de décision où les détenteurs de jetons ont le pouvoir d'influencer les règles, le développement et la gestion d'un protocole de finance.

Malgré son potentiel de décentralisation et de démocratisation, la gouvernance basée sur les jetons a son lot de problèmes :

- risque de centralisation si présence de gros détenteurs
- faible participation en raison d'un manque d'incitations ou à une connaissance insuffisante des enjeux de la plateforme
- manque d'expertise des détenteurs de jetons
- prise de décision lente, publique, parfois incohérente

La Defi est-elle décentralisée ?

La décentralisation d'un protocole est un processus complexe, multi-dimensionnel, long et progressif.

La plupart des protocoles defi ont des points de centralité (développeurs, fondateurs, interface, ...) mais ont comme objectifs de moyen terme une décentralisation accrue.

Réf : 1