Blockchain

Cours

Master 2 La Sorbonne Université

1

Description d'Ethereum

La blockchain Ethereum 1/4

La blockchain Ethereum est **différente de la blockchain Bitcoin**. Sur cette blockchain, les utilisateurs possèdent des comptes.

Il existe deux types de comptes :

1. Les « externally owned accounts » possédés et gérés par des utilisateurs
2. Les « contract accounts » gérés par un code informatique correspondant aux opérations que doit effectuer le contrat en fonction de l'état de la blockchain

La blockchain Ethereum 2/4

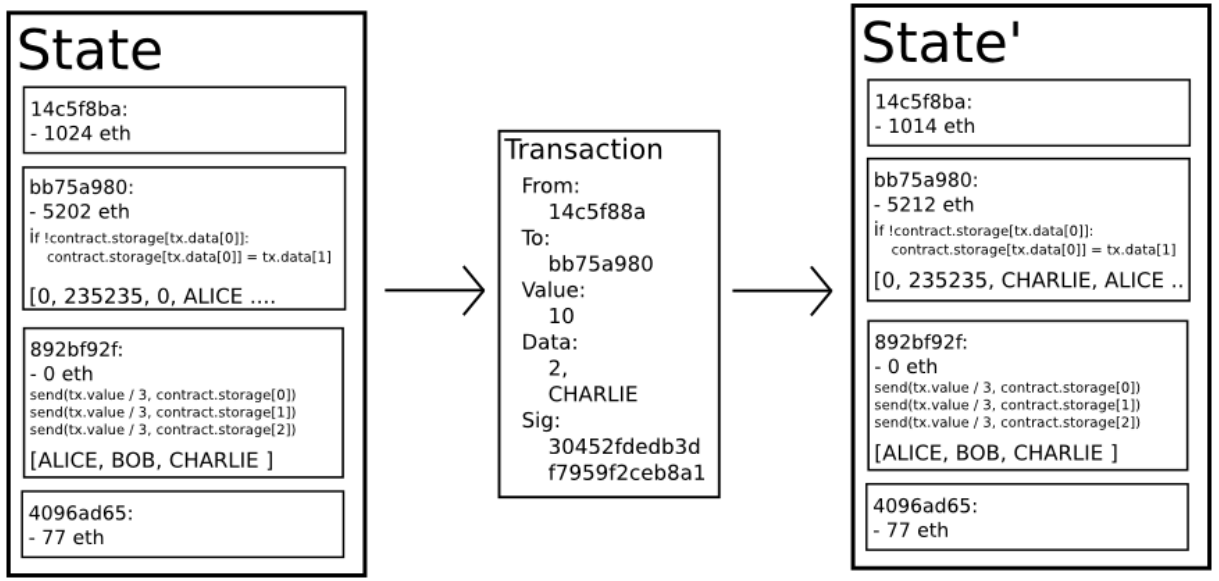
Le fonctionnement des « **externally owned accounts** » est assez similaire au fonctionnement des paires clé privée-clé publique sur la blockchain Bitcoin.

A l'inverse, les « **contract accounts** » représentent une grande nouveauté par rapport au Bitcoin. A chaque fois que ce type de compte reçoit une transaction, ***son code s'exécute en prenant cette transaction en input*** et peut lire et éditer son stockage interne, envoyer d'autres transactions sur la blockchain ou encore créer de nouveaux contract accounts.

La blockchain Ethereum 3/4

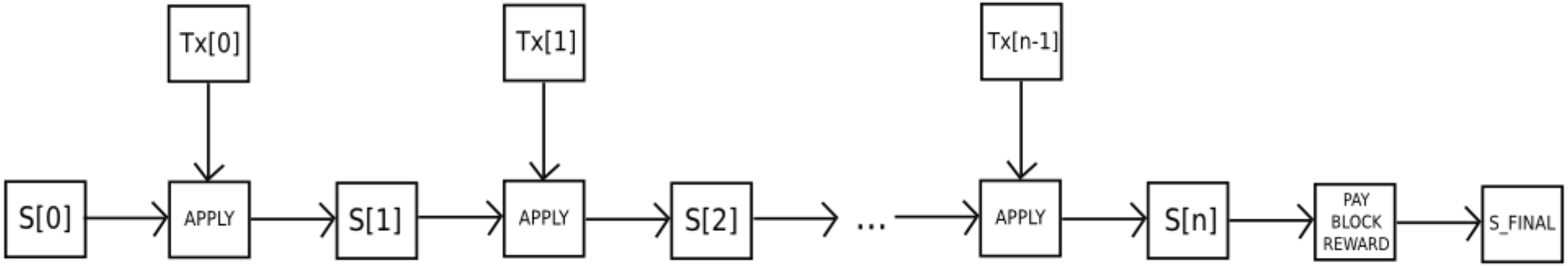
Les contrats présents sur la blockchain Ethereum sont donc **des entités autonomes hébergées par cette blockchain** qui gèrent leur stockage, leur stock d'ethers et leurs clés privées et exécutent systématiquement le même code à la réception d'une transaction.

Concernant la structure de la base de donnée Ethereum, **chaque bloc de la blockchain contient l'état du système**, c'est-à-dire l'ensemble des comptes avec leurs informations et leurs stocks d'ethers ainsi que les transactions en attente envoyées par les utilisateurs.



La blockchain Ethereum 4/4

La **transition** entre ces états consiste en l'envoi des transactions en attente et en la modification de tous les comptes concernés.



Proof of Stake : l'algorithme de consensus d'Ethereum 1/2

- Ethereum est passé du Proof of Work au Proof of Stake le 15 septembre 2022 suite à la finalisation du projet **"The Merge".**
- Ethereum se base sur le proof-of-stake, où des validateurs "stakent" des ETH qui sont bloqués dans un smart contract et peuvent être détruits si le validateur est jugé "malhonnête" ou "feignant". Le validateur doit vérifier la validité des blocs proposés au réseau et doit de temps en temps, au pro rata de ce qu'il stake par rapport aux autres, créer et proposer de nouveaux blocs.
- Pour participer comme validateur, un staker doit bloquer 32 ETH et faire tourner des softwares.
- Une fois les ETH stakés, l'utilisateur rejoint une "**queue d'activation**" qui limite le nombre de nouveaux validateurs rejoignant le réseau.
- Une fois "activé", le validateur est chargé de s'assurer de la validité de chaque nouveau bloc et dans ce cas de délivrer **une attestation**.
- Ethereum est actualisé par slots (12 secondes) et époques (32 slots, soit 384 secondes ou 6'24''). Un validateur est choisi aléatoirement à chaque slot pour proposer un nouveau bloc. Un comité de validateurs est également choisi aléatoirement pour determiner la validité du nouveau bloc proposé, selon les attestations qu'ils ont proposées.

Proof of Stake : l'algorithme de consensus d'Ethereum 2/2

- **Le premier bloc de chaque époque est un "checkpoint".**
- Les validateurs votent pour des paires de checkpoints considérés valides. Si plus des 2/3 des ETH stakés votent pour une paire de checkpoints, les checkpoints sont mis à jour. Le plus récent des 2 (la "**target**") devient "**justifié**". Le plus ancien de la paire est déjà jusitifié puisque c'était préalablement la target. Il devient donc "**finalisé**".
- Pour modifier un checkpoint finalisé, un attaquant doit risquer au moins 1/3 des ETH stakés.
- Ainsi, on considère qu'une transaction est "quasiment définitive" une fois qu'elle a été ajoutée dans un bloc inclu dans un checkpoint.
- Pour éviter qu'un attaquant ayant >1/3 des ETH stakés puisse bloquer toute validation de checkpoint, un mécanisme dit "**inactivity leak**" s'active si plus de 4 époques n'ont pas été validées. Durant une telle période, les ETH stakés par ceux qui ne votent pas comme la majorité sont progressivement détruits. Il faut donc >1/2 des ETH stakés pour empêcher des actualisations de checkpoints, puisqu'avec entre 1/3 et 1/2 des ETH stakés un attaquant perdrait progressivement des ETH jusqu'à actualisation des checkpoints.
- **Les validateurs sont rémunérés en ETH, mais leurs rewards peuvent être perdus** s'ils ne font pas ce qui est attendu d'eux. Les principaux comportements sanctionnés sont la proposition de plusieurs blocs ou l'émission d'attestations contradictoires.

2

Le système de gas d'Ethereum

Introduction

Ethereum est une plateforme qui **permet à des applications d'être exécutées de manière décentralisée et systématique**.

Pour cela, les applications sont exécutées sur un « ordinateur global » constitué par l'ensemble des ordinateurs interconnectés du réseau peer-to-peer.

L'application s'exécute de la même manière sur tous les ordinateurs du réseau par l'utilisation de ***l'Ethereum Virtual Machine***, qui peut effectuer des calculs et stocker des données.

Contrainte : l'exécution du programme doit être **déterministe** sinon les différents nœuds du réseau exécutant le programme se retrouveront avec une chaîne différente.

Les opérations ayant lieu sur le réseau Ethereum sont composées de transactions, la transaction étant la brique élémentaire des actions réalisées sur le réseau Ethereum.

Qu'est-ce que le gas? 1/2

Le « gas » est une crypto-monnaie au même titre que l'ether, qui n'est cependant **utilisée que lors de l'exécution d'applications sur le réseau Ethereum**. C'est, métaphoriquement, *le carburant* qui permet aux applications de s'exécuter.

L'exécution d'une application sur le réseau Ethereum peut être vue comme un trajet en voiture. De même que la quantité de carburant à utiliser pour un trajet en voiture dépend de la longueur du trajet, la quantité de gas à utiliser pour exécuter une application Ethereum **dépend de la longueur d'exécution de l'application** (donc de sa complexité algorithmique). Chaque opération de l'Ethereum Virtual Machine a un coût en gas.

Plus le programme utilise de stockage et de puissance de calcul, plus le montant de gas à fournir pour son exécution est élevé. Lors de la création d'une transaction, l'émetteur fixe un plafond correspondant au montant de gas maximum que la transaction est autorisée à consommer. Le terme consacré pour désigner ce plafond est **STARTGAS**.

Qu'est-ce que le gas? 2/2

Pour que le système fonctionne correctement, **il est nécessaire qu'un startgas soit spécifié**. Ceci est dû au fait que, la plupart du temps, il est impossible pour le staker de savoir combien de temps requerra une transaction avant de l'exécuter, ou même de savoir si celle-ci s'exécutera en temps fini (**halting problem**).

Il existe des outils pour estimer le startgas nécessaire à l'exécution d'une transaction.

Le passage de l'ether au gas, comme tout échange de devises, est soumis à un taux de change, dont le nom est **GASPRICE**.

Le gasprice est fixé par **l'émetteur de la transaction**.

Operation Name	Gas Cost	Remark
step	1	default amount per execution cycle
stop	0	free
suicide	0	free
sha3	20	
sload	20	get from permanent storage
sstore	100	put into permanent storage
balance	20	
create	100	contract creation
call	20	initiating a read-only call
memory	1	every additional word when expanding memory
txdata	5	every byte of data or code for a transaction
transaction	500	base fee transaction
contract creation	53000	changed in homestead from 21000

Emission d'une transaction

Lors de l'émission d'une transaction, l'utilisateur envoie sa transaction sur le réseau peer-to-peer et spécifie un **STARTGAS** ainsi qu'un **GASPRICE** qu'il fixe lui-même. Le produit **STARTGAS**x**GASPRICE** correspond au **fee**, à savoir la somme maximale **en ether** qui va être déboursée par l'utilisateur afin d'exécuter sa transaction.

Le **fee** correspond à la somme maximale que l'émetteur est prêt à dépenser pour faire exécuter sa transaction. A l'issue de l'exécution de la transaction, ***le gas utilisé par l'exécution est versé au staker ayant miné le bloc dans lequel la transaction est inclue***.

Le staker **convertit alors ce gas en ether** et empoche la somme. Le gas non utilisé est converti lui aussi en ether et est reversé à l'émetteur de la transaction.

Si le gas fourni par l'utilisateur n'est pas suffisant pour exécuter la transaction, le staker ayant inclu cette transaction dans un bloc empoche le **fee** dans son intégralité, la transaction est inclue dans le bloc **mais n'effectue aucune modification du système** (le système revient à son état pré-transaction).

GASPRICE

Le taux de change ether-gas, ou **GASPRICE** est fixé **par l'utilisateur**. Cependant, pour être exécutée, la transaction doit être prise en charge et inclue dans un bloc par un staker, qui engage lui-même une dépense en électricité et matériel informatique afin de miner efficacement.

Afin de rentabiliser leur activité, les stakers fixent donc eux-mêmes un **GASPRICE** minimal en dessous duquel les transactions qui leurs sont envoyées ne sont pas inclues dans un bloc.

Le **GASPRICE** minimum accepté dépend de chaque staker.

Malgré le fait que le **GASPRICE** (propre à chaque transaction) soit fixé par l'émetteur de la transaction, les stakers ont un rôle à jouer dans l'établissement de ce prix par le seuil minimal qu'ils fixent.

Ce **GASPRICE** étant un taux de change, il est également impacté par le prix de l'ether. Si le prix de l'ether monte, le **GASPRICE** doit être ajusté afin de ne pas rendre le coût des transactions et de l'exécution des applications trop important.

Gas refund 1/3

- Si on fait l'hypothèse que tous les émetteurs de transactions utiliseront le seuil minimum de gasprice des stakers comme gasprice, on peut considérer que ***les stakers fixent eux-mêmes le taux de change ether-gas***. Sous cette hypothèse, le taux de change ether-gas est alors déterminé par la distribution des seuils minimum de gasprice fixés par les stakers du réseau Ethereum
- **Gas refund** : en parallèle du compteur de gas disponible pour l'exécution d'une transaction, qui a une valeur initiale égale au startgas, il existe un compteur de ***gas refund***. En libérant de l'espace de stockage ou en supprimant un contrat stocké sur la blockchain Ethereum, un utilisateur a le droit à un refund de gas lors de la transaction effectuant ces opérations. Le compteur de refund gas est parallèle au compteur de gas disponible car si le compteur de gas disponible tombe à zéro, une « **out of gas exception** » est déclenchée et ***la transaction est inclue dans un bloc sans que son contenu soit exécuté***, et ce même si le refund gas n'est pas à zéro.
- **Cet aspect doit affecter le taux de change ether-gas.**

Gas refund 2/3

- Afin de pouvoir utiliser le gas refund, ***une transaction doit donc contenir initialement suffisamment de gas pour être executée***.
- **Le refund est au plus égal à la moitié du gas utilisé**. Ceci permet à un staker qui inclut une transaction contenant du gas refund (voire une transaction à solde négatif) d'être tout de même rémunéré pour son travail. Cela pousse donc les stakers à ne pas écarter les transactions contenant beaucoup de gas refund.
- Les blocs de la blockchain Ethereum sont limités en startgas. En effet, pour qu'un nouveau bloc soit vérifié, il doit être exécuté par les membres du réseau P2P. Pour que la charge de calcul nécessaire à la vérification d'un nouveau bloc ne soit pas trop importante, on limite ainsi sa taille en terme de startgas, qui représente une estimation de la complexité d'exécution de la transaction faite par son émetteur.
- Ceci est appelé la **Block Gas Limit** (BGL).

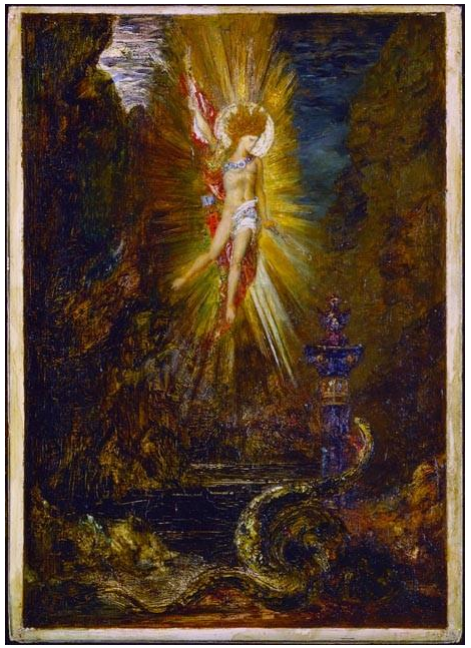
Gas refund 3/3

- Pourquoi ne pas fixer une startgas très élevée, par exemple égal à 3M?
  A cause de la stratégie des stakers.
- Lors de l'exécution d'une transaction, le staker ne reçoit pas le startgas mais seulement le gas utilisé par la transaction.
- En voyant un startgas très élevé, un staker se doutera que le gas utilisé par la transaction est surestimé et qu'il n'empochera pas les 3M. Il préfèrera inclure 100 transactions ayant un startgas égal à 30000
- Un staker aura tendance à privilégier un ensemble de transactions ayant un startgas raisonnable plutôt qu'une transaction unique ayant un startgas très élevé.
- A cause de cette stratégie des stakers, une transaction ayant un startgas très élevé ne sera pas inclue en priorité dans la blockchain et pourra mettre un peu de temps à être exécutée. Il est donc préférable de **bien estimer la complexité de calcul de la transaction et de fixer une startgas raisonnable**. On voit ainsi ***de nouvelles problématiques d'analyses quantitatives*** émerger.

Un aspect important : ***les oracles***

IMPOSSIBLE PAR SMART CONTRACT :

Parier sur le costume que portera Mr X à une réunion…



IL FAUT EXTRAIRE DES DONNEES FIABLES QUI DETERMINENT LES CLAUSES :

Ces données n'étant pas contenues dans la blockchain, on parle d'*oracle*

Il existe 3 types d'oracles :

- **Les oracles web (exemple : l'equipe.fr pour un pari sportif)**
- **Les oracles consensuels (exemple Bletcheley)**
- **Les oracles locaux (exemple database pour extraire le taux Libor)**

3

Tokens & Initial Coin Offering (ICO)

Un moyen de représentation des actifs : le token

- Un **token** est une entité digitale représentée sur une blockchain et représentant un actif physique ou virtuel.
- Il peut s'échanger rapidement **sans intermédiaire** par une blockchain.
- Un token peut représenter un actif **fongible ou non fongible**.
- Un actif fongible est un actif composé d'unités qui sont indistinguables et interchangeables (exemples : lingots d'or, billets de banque…).
- Un actif non fongible est composé d'unités distinctes et non-interchangeable (exemple : La Joconde est unique malgré l'existence de copies). Un tel actif peut être représenté par un token et on parle alors de **NFT (Non-Fungible Token)**. Il existe notamment des NFTs représentant des œuvres d'art digitales ou des certifications de propriétés d'actifs tangibles.

Définition des ICOs

- Une Initial Coin Offering (ou ICO) est une opération de levée de fond participative publique basée sur la blockchain, à la croisée des chemins entre le "crowdfunding" et l'Initial Public Offering (IPO).
- En effet, lors d'une ICO, l'entité cherchant à recueillir des financements crée un nouveau token sur une blockchain, nouvelle ou préexistante, et le propose à la vente pendant une période de temps donnée.
- Contrairement au cas d'une opération de "crowdfunding" standard, l'investissement dans une ICO est une opération d'achat, l'investisseur échangeant véritablement une crypto-monnaie ou une monnaie fiat contre des tokens de l'ICO.
- Ceci rapproche l'opération d'ICO de l'opération d'IPO. Cependant, une différence très importante existe entre ces deux processus. Contrairement à des actions d'entreprises, les tokens achetés lors d'une ICO n'accordent pas nécessairement de droits sur les bénéfices de l'entité émettrice et n'accorde pas nécessairement de droit de décision ou de vote.
- Les propriétés d'un token dépendent de la blockchain sur laquelle il est développé (limitations technologiques), de la volonté de son émetteur, de la nature de son projet et de la régulation, dépendante de sa nature, qui encadrera l'usage de ce token. Un token d'ICO peut avoir les propriétés d'une action, accorder un droit de vote, servir une fonction particulière dans le projet mis en place ou n'avoir aucune utilité.

Le standard de token ERC20 1/2

La blockchain Ethereum offre la possibilité aux utilisateurs de créer leur token. Les tokens créés par les utilisateurs dépendent alors de la blockchain Ethereum et fonctionnent comme une surcouche de ce système.
Le standard ERC20, pour “Ethereum Request for Comments 20”, est une classe virtuelle de contrat de token contenant les fonctions et informations qui doivent être présentes dans le contrat d’un token présent sur la blockchain Ethereum afin que celui-ci puisse être considéré comme un token ERC20 :

```
1 contract ERC20Interface {
2     function totalSupply() public constant returns (uint);
3     function balanceOf(address tokenOwner) public constant returns (uint balance);
4     function allowance(address tokenOwner, address spender) public constant returns (uint remaining);
5     function transfer(address to, uint tokens) public returns (bool success);
6     function approve(address spender, uint tokens) public returns (bool success);
7     function transferFrom(address from, address to, uint tokens) public returns (bool success);
8
9     event Transfer(address indexed from, address indexed to, uint tokens);
10     event Approval(address indexed tokenOwner, address indexed spender, uint tokens);
11 }
```

Le fonctionnement du standard ERC20 étant connu, l’utilisation de ce type de tokens permet une uniformisation des tokens présents sur la blockchain Ethereum et une meilleur connaissance de leur comportement sur cette blockchain.
Parmi les tokens émis lors des ICOs récentes, nombreux sont ceux qui respectent le standard ERC20.

Le standard de token ERC20 2/2

L'architecture de contrat du token ERC 20 définit 6 fonctions :

- **function** totalSupply() **public** constant returns (uint)

  Fonction renvoyant le nombre total de token en circulation.

- **function** balanceOf(address tokenOwner) **public** constant returns (uint balance)

  Fonction prenant l'adresse d'un utilisateur et renvoyant le nombre total de tokens en sa possession.

- **function** allowance(address tokenOwner, address spender) **public** constant returns (uint remaining)

  Fonction prenant l'adresse d'un propriétaire de tokens et d'un destinataire et renvoyant le nombre de tokens que le destinataire est autorisé à prélever au propriétaire. **Cette autorisation peut concerner un autre utilisateur ou un smart contrat.**

- **function** transfer(address to, uint tokens) **public** returns (bool success)

  Fonction prenant une adresse de destination et un nombre de token et renvoyant un booléen représentant le succès ou l'échec de la transaction. Cette fonction permet à un utilisateur de la blockchain Ethereum d'envoyer ses tokens à d'autres utilisateurs.

- **function** approve(address spender, uint tokens) **public** returns (bool success)

  Fonction prenant l'adresse d'un destinataire et un nombre de tokens et renvoyant un booléen représentant le succès ou l'échec de l'opération. **Cette fonction permet à un utilisateur de la blockchain Ethereum d'autoriser un autre utilisateur ou un smart contrat à prélever un certain nombre des tokens qui sont en sa possession. A chaque appel, cette fonction réécrit la variable renvoyée par la fonction** allowance**.**

- **function** transferFrom(address from, address to, uint tokens) **public** returns (bool success)

  Fonction prenant l'adresse d'un propriétaire de tokens, d'un destinataire ainsi qu'un nombre de tokens et renvoyant un booléen représentant le succès ou l'échec de l'opération. **Cette fonction permet à un utilisateur d'autoriser un smart contrat à envoyer des tokens à sa place à un destinataire (utilisateur ou autre smart contrat).**

Comment fixer la valeur d'un token d'ICO?

C'est un problème complexe et loin d'être résolu ….

- La manière la plus pertinente de fixer le taux de change du token émis lors d'une ICO est de fixer la valeur du token en monnaie fiat et de choisir un taux de change avec une autre crypto-monnaie en fonction de cette valeur. Une fois ce taux de change fixé, par exemple un taux de change token/BTC, la valeur effective du nouveau token émis dépendra de l'évolution du prix du BTC.
- La valeur du token en monnaie fiat peut donc être fixée longtemps avant l'ICO et dépendra de la nature du projet (communauté d'utilisateurs, utilisation du token par l'application ou non) et des prévisions d'utilisation du token et de spéculation faites par l'équipe en charge du projet (à éclaircir et préciser)
- Le taux de change token/BTC devra en revanche être fixé très peu de temps avant l'ICO et l'ICO devra de préférence être réalisée en période de faible volatilité sur le marché du BTC. Sinon, la valeur effective des nouveaux tokens en fiat money pourra fortement varier.
- Deux manières systématiques de fixer la valeur des tokens en fiat :
  - *Calcul stochastique* :
    - http://news.8btc.com/pboc-official-research-on-ico-and-its-regulation
  - *Théories économiques monétaires :*
    - http://www.bankofcanada.ca/wp-content/uploads/2016/08/swp2016-42.pdf
    - https://basicattentiontoken.org/BasicAttentionTokenWhitePaper-4.pdf
    - "Fundamental Pricing of Utility Tokens" de Julien Prat, Vincent Danos et Stefania Marcassa

Pricing par calcul stochastique d'un token d'ICO

- Un début de méthode de pricing de tokens émis lors d'une ICO a été réalisé par le PBOC Digital Currency Research Institute (People's Bank of China). La documentation manque un peu sur cette méthode de pricing.
- Les auteurs souhaitent pricer les tokens émis lors d'une ICO comme une option sur la valeur du projet développé exprimée en BTC:
  - Valeur du projet dans le futur : $S(T)$
  - Valeur du Bitcoin à cette date : $U(T)$
  - Valeur du projet à cette date en fiat money : $V(T) = S(T)U(T)$
  - Prix du token au temps T : $P(T) = (S(T) - Z)_+$ où Z est une valeur seuil exprimée en BTC
- Si la valeur du projet passe en dessous du seuil Z, on considère que celui-ci a raté et sa valeur la valeur du token associée est donc nulle. Cette hypothèse est un peu forte, un token pouvant avoir une valeur liée uniquement à la spéculation.
- Si le temps de mise en place de l'ICO est le temps 0, déterminer le taux de change token/BTC à fixer revient à calculer le prix du token au temps initial $P(0)$.
- Afin de déterminer ce prix, les auteurs utilisent la méthode standard de pricing d'options, en faisant l'hypothèse que la valeur du projet $S(t)$ évolue selon un mouvement Brownien géométrique (modèle de Black-Scholes). Cette hypothèse est discutable, la valeur du projet devrait être estimée de manière très précise et systématique et à des dates très rapprochées pour voir si celle si peut être modélisée par un mouvement Brownien. Pour l'instant, les auteurs ne justifient pas de choix (celui permet évidemment de donner une formule de prix sans avoir à de calcul ou d'exercice de modélisation) et ne l'étayent pas par des données.
- Les résultats obtenus par les auteurs sont les suivants :
  - $P(0) = \frac{V(0)}{U(0)} e^{-q_v T} N(d_1) - e^{-q_u T} N(d_2) - 1$ avec $S(T) = \frac{V(T)}{U(T)}$ et en posant $Z = 1$
  - $d_1 = \frac{\ln\left(\frac{V(0)}{U(0)}\right) + \left(q_u - q_v + \frac{\sigma^2}{2}\right)T}{\sigma\sqrt{T}}$
  - $d_2 = d_1 - \sigma\sqrt{T}$
  - $\sigma = \sqrt{\sigma_u^2 - \sigma_v^2 - 2\rho\sigma_u\sigma_v}$
  - Où q_v est le taux de croissance de la valeur du projet, q_u est le taux de croissance de la valeur du Bitcoin, et σ_v et σ_u sont les volatilités associées.

Pricing par méthodes économiques d'un token d'ICO

- Dans l'article « *On the value of virtual currencies* », Bolt et van Oordt développent une théorie monétaire afin de modéliser le taux de change entre une monnaie « standard » (par exemple l'euro), et une crypto-monnaie (par exemple le bitcoin).
- Leur modélisation prend en compte :
  - La « vélocité » de la monnaie, définie comme le nombre moyen de fois qu'une monnaie est utilisée afin d'acheter un bien ou un service au cours d'une période t. Notée V_t^B pour le Bitcoin.
  - La quantité de biens ou services achetés à l'aide de la monnaie pendant une période t. Notée T_t^B pour le Bitcoin.
  - La prix moyen de ces biens. Noté P_t^B pour le Bitcoin.
  - La quantité nominale de monnaie émise. Notée M_t^B pour le Bitcoin.
  - La masse monétaire impliquée dans la spéculation. Notée Z_t^B pour le Bitcoin.
- Le point de départ de l'article est la « quantity equation » de Fisher (1911) : $P_t^B T_t^B = M_t^B V_t^B$
- En posant T_t^{B*} la quantité de biens ou services achetés en cryptomonnaie, exprimée en monnaie fiat, on a : $\frac{P_t^B}{P_t^\$} T_t^{B*} = M_t^B V_t^B$
- Les auteurs font ensuite apparaître le taux de change crypto-dollar $S_t^{\$/B} = \frac{P_t^\$}{P_t^B}$ afin d'exprimer celui-ci en terme des quantités présentées ci-dessus : $S_t^{\$/B} = \frac{T_t^{B*}}{M_t^B V_t^B}$
- Ils expriment la vélocité comme une moyenne de la vélocité de la masse financière utilisée pour acheter des biens et des services V_t^{B*} et de la vélocité financière stockée pour des raisons spéculatives, qui est nulle : $V_t^B = \frac{M_t^B - Z_t^B}{M_t^B} V_t^{B*} + \frac{Z_t^B}{M_t^B} 0$
- Le taux de change dollar-Bitcoin peut alors être exprimé en fonction de la quantité de biens et services achetés en Bitcoin exprimée en dollars, de la masse monétaire totale, de la masse monétaire impliquée dans la spéculation (considérée comme immobile ainsi que de la vélocité de la masse de Bitcoin utilisée pour acheter des biens et services : $S_t^{\$/B} = \frac{T_t^{B*}}{(M_t^B - Z_t^B) V_t^{B*}}$
- Ceci forme la base de la méthode développée par les auteurs. A cela s'ajoute des développements raffinant le modèle.

Description d'ICOs

Q3 2014

Levée de fonds pour

ethereum

En échange de

bitcoin

1. ***Date de l'ICO:*** 22 juillet -> 2 septembre 2014
2. ***Montant levé***: 31 500 BTC – 18,4 M $ à cette époque
3. **Méthode d'émission**: Non capé mais avec une date de fin d'émission
4. **Mécanisme de vente:** Le taux d'échange diminuait linéairement allant de 2000 ETH par BTC à 1337 ETH pour 1 BTC

Avantages:

- Première grosse levée de fonds
- La stratégie de communication a permis une bonne compréhension de la technologie
- Le succès de cette ICO a eu une fort impact pour la communauté des crypto-monnaie.

Inconvénients:

- Les délais n'ont pas été tenus et ont conduit à repousser plusieurs fois le projet
- Il était difficile pour les investisseurs d'aller au bout du process

Q4 2015

Levée de fonds pour

IOTA

En échange de

bitcoin

1. ***Date de l'ICO:*** 25 Novembre -> 21 décembre 2015
2. ***Montant levé***: 1337 BTC – 584 K $ à cette époque
3. **Méthode d'émission**: L'intégralité des 999 999 999 iotas étaient en vente
4. **Mécanisme de vente:** Pas de taux d'échange mais un système proportionnel 10% de tous les bitcoin = 10% de tous les IOTA

Avantages:

- Méthode de levée de fond innovante
- Projet ambitieux

Inconvénients:

- Communication limitée avec un white paper incomplet: une partie de la communauté pensait que c'était un scam.
- Problèmes de sécurité : Les fonds collectés n'étaient pas verrouillés dans un multi-sig wallet

Focus sur l'ICO de BAT

- **Cryptos acceptées pendant l'ICO :** uniquement ETH
- **Volume :** 1 milliard de BAT mis en vente + contrat avec 300 millions de BAT (« user growth pool », pour inciter les nouveaux utilisateurs) et 66.35 millions de BAT (« development pool », pour l'équipe de développeurs) + contrat verrouillé pendant 180 jours contenant 133,650,000 BAT
- **Prix** : 1 ETH pour 6400 BAT. L'objectif de recette de l'ICO a été fixé en dollars. Le taux de change ETH/BAT et le nombre de BAT mis en vente ont donc été fixés afin de pouvoir atteindre l'objectif de recette. Ce prix a été estimé par un raisonnement économique présenté dans le whitepaper de l'équipe, et dérivé de celui réalisé dans l'article *On the value of virtual currencies*, de Bolt et van Oordt (Bank of Canada)
- **Recettes :** 1 milliard de BAT vendus pour un total de 156,250 ETH (36,064,062 dollars au 31/05/2017, jour de l'ICO selon Coinbase)
- **Répartition des token :** la « user growth pool » sert à récompenser les nouveaux utilisateurs de BAT par un versement de token, fonctionnement pas encore fixé. La « development pool » sert à récompenser les développeurs ne faisant pas partie de l'équipe mais participant au développement du projet sur github. ETH reçus stockés sur un wallet multi-sig.
- **Token listé sur plateformes d'échange? :** oui
- BAT/LTC et BAT/DOGE sur Cryptopia, BAT/BTC et BAT/ETH sur Bittrex, BAT/CNY sur Bter
- **Nature du token :** les BAT sont utilisés dans l'application, un utilisateur devra payer des BAT pour pouvoir utiliser les services de l'application, la possession de BAT fournit donc un avantage stratégique quelque soit la volonté de l'utilisateur (spéculation ou volonté d'utiliser la plateforme)
- **Exemples d'utilisation :** versements de BAT pour obtenir du contenu premium de la part des éditeurs, donations aux éditeurs
- **Bilan :** l'ICO de BAT s'est achevée en 30 secondes. Ceci a eu pour conséquence de créer une « course au fees ». Une sorte d'enchère a eu lieu où les investisseurs mettant le plus de transactions fees pouvaient obtenir leur tokens. La congestion du réseau Ethereum et la vitesse de vente de ces BATs a empêché les investisseurs n'ayant pas proposé des frais de transactions suffisamment élevés aux mineurs ou ne possédant pas un full node (propagation de la transaction plus lente pour les utilisateurs ne possédant pas de full node) d'obtenir des BATs. Au total, seulement ***190 utilisateurs*** environ ont pu participer à cette ICO très attendue, dont une majorité de gros investisseurs. Un mécanisme de limitation de gas aurait peut être permis d'éviter cette course au gas pour que la transaction puisse passer. A noter, la capacité de la blockchain Ethereum était pleine pendant les 3 heures suivant le début de l'ICO.

4

Finance décentralisée (DeFi)

Un sujet émergent : la finance décentralisée (DeFi)

- **Définition :** La finance décentralisée (Decentralized Finance, ou DeFi) est une forme de finance qui n'utilise pas d'intermédiaires tels que les banques, les brokers ou les plateformes d'échange, mais qui se basent sur l'utilisation de smart contracts mettant en relation les parties directement de façon pair à pair.
- **Taille de marché** : Plusieurs dizaines de milliards de dollars stockés dans les contrats de DeFi en 2021
- **Stablecoin** : Représentation par un actif digital d'un autre actif. C'est souvent une monnaie fiat, majoritairement le dollar, mais ça peut aussi être des commodities comme l'or. Les principaux sont Tether (USDT), USD Coin (USDC), Binance USD (BUSD) et le DAI qui est algorithmique.
- **DEX** (exchanges décentralisés) : plateformes d'échanges d'actifs digitaux pair à pair, sans tiers de confiance. Il arrive cependant que le trading soit basé sur des tiers de confiance, notamment par exemple quand ce sont des stablecoins ou des représentations sur une blockchain d'une cryptomonnaie ou d'un token qui a été déployée sur une autre blockchain (on parle de « wrapped assets »).
- **Exemples de projets :** Uniswap, Maker, Sushiswap, Yearn finance, Aave, Ribbon…

Focus sur Maker et le DAI 1/2

- Initié en 2015 et lancé fin 2017, **MakerDAO propose une solution alternative et ne reposant pas sur le monde physique ou sur une autorité centrale : un système analogue à la mise en gage d'un objet en échange d'un prêt**.
- Dans le cas de MakerDAO, l'objet qui est mis en gage dans un « Maker Vault » est un crypto-actif, et **le prêt est exprimé dans une cryptomonnaie créée pour l'occasion** et dont le cours ne fluctue pas et est censée être un stablecoin dollar, le DAI. L'entité qui conservait le crypto-actif mis en gage était un smart contract appelé **Collateralized Debt Position (CDP)**, que seul le créancier a la possibilité de débloquer. Désormais, ces mécanismes sont regroupés sous la forme du « Multi-Collateral Dai »(MCD).
- La valeur du stablecoin DAI, pour qu'elle soit considérée comme constante, doit être garantie par le fait que le collatéral en vaut toujours au moins le montant équivalent à ce qui a été emprunté. Pendant plusieurs années, seul l'ETH pouvait être utilisé comme collatéral, même si d'autres sous-jacents sont désormais envisageables, aujourd'hui tout actif représenté sur Ethereum approuvé par la gouvernance de Maker. La Société Générale a par exemple proposé un security token comme garantie pour un prêt de 20 millions de dollars en 2021 (source : https://cryptonaute.fr/societe-generale-sessaye-a-la-defi-avec-un-pret-en-dai-sur-ethereum/).
- La valeur des collatéraux des prêts étant fluctuante, il est possible que la valeur du collatéral devienne inférieure au montant du prêt correspondant. L'emprunteur n'aurait alors plus aucun intérêt à rembourser son prêt et le système s'écroulerait. C'est pourquoi **un mécanisme de sécurité** est mis en place : **la collatéralisation de chaque prêt ne peut jamais descendre en dessous d'un ratio, le Liquidation Ratio, décidé par vote et dépendant de la nature du collatéral**. Pour ETH, il a été de 150% puis de 200%. Si le cours d'un collatéral descend au niveau de ce ratio, un processus de liquidation s'active dans le cadre d'une « collateral auction » pour équilibrer la situation. L'information du cours des collatéraux est obtenue **grâce à des oracles dédiés**.
- MakerDAO a mis en place **deux tokens spécifiques** : le Dai (DAI) et le Maker (ou MKR), un token permettant à ses possesseurs de voter, et donc de participer à la gouvernance du projet MakerDAO.
- Chaque prêt en DAI présente **un Stability Fee** dépendant de la nature du collatéral (1% à 10%), payable en DAI.

Focus sur Maker et le DAI 2/2

- Le **Dai Savings Rate (DSR)** permet à tout détenteur de Dai de percevoir des intérêts automatiquement par smart contract en bloquant ses Dai dans le contrat DSR du protocole Maker.
- Le contrat DSR est **un système global qui détermine le taux d'intérêt obtenu par les détenteurs de Dai** au fil du temps. Quand le prix de marché du Dai dévie du "Target Price" (1$), les détenteurs de tokens MKR peuvent decider par vote de modifier le DSR :

a) Si le prix du Dai est supérieur à 1$, les détenteurs de MKR peuvent choisir de baisser le DSR, ce qui devrait réduire la demande et rapprocher le prix du Dai de 1$.

b) Si le prix du Dai est inférieur à 1$, les détenteurs de MKR peuvent choisir d'augmenter le DSR, ce qui devrait augmenter la demande et rapprocher le prix du Dai de 1$.

- Le système MakerDAO présente plusieurs autres mécanismes de sécurité garantissant la collatéralisation, notamment la possibilité pour les détenteurs de MKR de voter un « **Emergency Shutdown** » qui a 3 phases :

1. Le protocole Maker ferme et les détenteurs de Vault retirent leurs actifs.
2. Une auction dite « Post-Emergency Shutdown » est déclenchée.
3. Les détenteurs de Dai obtiennent leur parts des collatéraux restants.

- La Maker Foundation qui a construit et lancé le protocole Maker**, a pour objectif de rendre la gouvernance décentralisée puis de se dissoudre** une fois que la gouvernance mise en place sera suffisante pour le projet. Ce projet deviendra alors une DAO (Decentralized Autonomous Organization).
- Le 12 mars 2020, un crash de marché a eu lieu sur l'ETH et la blockchain Ethereum a été congestionnée. Cela a entraîné des liquidations de collatéraux de CDPs que certains ont obtenu gratuitement (c'était avant la mutualisation par le MCD) à cause de la courte période accordée aux auctions. Ceci a entraîné une perte de valeur pour les détenteurs de MKR. Il y a eu ensuite une class action de certains utilisateurs contre la foundation Maker pour "représentation intentionnellement biaisée des risques associés à la détention de CDP". Source : https://www.coindesk.com/tech/2020/04/14/makerdao-users-sue-stablecoin-issuer-following-black-thursday-losses/

Focus sur Aave 1/2

- Né en 2017 après une ICO de 16 millions de dollars avec notamment Stani Kulechov, un juriste et développeur finlandais
- Le protocole a commencé par proposer **des prêts en pair-à-pair sur Ethereum**. Il mettait directement en relation un emprunteur et un déposant. À travers un *smart contract*, l'emprunteur payait un intérêt au second. Des cryptomonnaies sont en garantie dans le cas où il ne serait pas capable de rembourser.

- **Les *pools* de liquidité**, soit des réserves mutualisées de cryptomonnaies, permettent une « industrialisation » sans rencontre directe entre prêteurs et emprunteurs. Les apporteurs de liquidité mettent en commun leurs cryptos et reçoivent les intérêts au prorata.
- Il n'y a pas d'entreprise qui contrôle le protocole. L'équipe de développement détient des jetons Aave (18% de la masse monétaire). Elle se rémunère comme n'importe quel détenteur de jetons en percevant une partie des frais prélevés sur chaque emprunt.
- Aave offre des emprunts à taux variables et à taux fixes.
- Aave propose des ***flash loans*** **:** ce sont des prêts ultra-rapides que l'on peut contracter sans apporter de garantie et rembourser en quelques secondes. Si l'emprunteur n'est pas en mesure d'honorer sa dette, l'ensemble des opérations sont annulées et le flash loan n'est pas intégré dans le prochain bloc validé de la blockchain.
- Aave propose également **de la délégation de crédit** : quelqu'un qui dépose des cryptos dans le protocole peut offrir sa capacité de crédit à d'autres utilisateurs qui ne seraient pas en mesure de présenter une garantie. Un peu comme si un ami se portait caution pour votre emprunt. En contrepartie, l'emprunteur est soumis à un taux un peu plus élevé pour rémunérer le délégateur.

Focus sur Aave 2/2

- Sur chaque prêt, les emprunteurs paient des frais (0,0000001% du montant emprunté, 0,09% pour les *flash loans*). Une grande majorité est reversée aux apporteurs de liquidité et aux détenteurs du jeton Aave. La partie minoritaire abonde **un fonds spécial (Reserve Factor)** dont l'allocation doit faire l'objet d'un vote parmi les détenteurs du jeton Aave. Elle peut aller au développement de nouvelles fonctionnalités ou bien être reversée aux détenteurs (de la même façon qu'un dividende).
- **Le jeton Aave** sert principalement à exercer la gouvernance du protocole. Chaque évolution (proposer des prêts sur une nouvelle cryptomonnaie par exemple) est soumise au vote de la communauté. Un jeton équivaut à une voix. **L'équipe de développement en détient 18%, des fonds de capital-risque autour de 3% et le reste est réparti parmi la communauté.**
- Il est possible de participer à la sécurisation du protocole **en immobilisant des jetons Aave dans le *Safety Module***. Ce mécanisme s'apparente à un fonds de sauvetage dans lequel on pioche si le protocole subit des pertes. Jusqu'à 30% des jetons peuvent être saisis. En contrepartie, ceux qui acceptent d'y participer sont rémunérés à un taux annuel avoisinant les 6%. Ce n'est que de cette façon que les détenteurs du jeton Aave peuvent bénéficier de la redistribution des frais de transaction. Avoir simplement des jetons dans un portefeuille ne procure aucun rendement.
- Les jetons peuvent être débloqués du *Safety Module* sous un délai de dix jours. Cela limite les risques de fuite des capitaux en cas de panique boursière.
- Les détenteurs du jeton Aave qui souhaitent du rendement peuvent également en immobiliser sur le protocole Balancer. **Cette deuxième réserve est programmée pour racheter automatiquement les jetons Aave du Safety Module dans le cas où le protocole subirait des pertes.**
- **L'ensemble de ces mécanismes d'incitation réduit la part de jetons disponibles à la vente**. Cela participe à la progression de sa valeur.

Focus sur Uniswap 1/5

- Uniswap est né d'une idée proposée par Vitalik Buterin, le cofondateur d'Ethereum, sur reddit en 2016.
- Cette idée a été reprise fin 2017 par Hayden Adams, fondateur d'Uniswap, pour la transformer en une application fonctionnelle. Le projet Uniswap a bénéficié d'une bourse de 100.000 dollars de la part de la Fondation Ethereum. **Sa première version opérationnelle a vu le jour en novembre 2018.**
- Uniswap est une plateforme d'échange décentralisée développée sur le protocole Ethereum. À la différence d'une bourse traditionnelle où les échanges sont certifiés par une entreprise, Uniswap (qui n'est qu'un programme informatique) met en relation des acheteurs et des vendeurs sans intermédiaire. Il n'est pas nécessaire de renseigner des informations personnelles (papiers d'identité, justificatif de domicile, etc.). Seul un portefeuille numérique chargé en cryptos est nécessaire.
- Son système utilise une innovation baptisée **Automated Market Making (AMM)** à la place d'un carnet d'ordres traditionnel.
- Il n'y a pas de carnet d'ordre mais une évolution des réserves x et y de la paire de jetons échangés tels que $x * y = k$ reste constant (k augmente en fait un peu avec les frais). Exemple : s'il y a $x = 100$ tokens A et $y = 200$ tokens B en réserve, un trader souhaitant trade $a = 20$ tokens A contre des tokens B recevra n tel que $(x + a) * (y - n) = x * y$, soit, en l'absence de frais :

$$n = \frac{a * y}{x + a} \approx 33.33$$

- En revanche, si $a = 1$ alors $n \approx 1{,}98$. Ainsi, pour un petit trade, il y a peu de slippage et le prix d'un trade correspond au rapport des réserves entre les 2 tokens. Plus le trade est important comparé aux réserves, plus il y a de slippage.
- Les AMMs ont typiquement 3 types d'acteurs :

1. **Les traders** échangent les tokens l'un contre l'autre.
2. **Les liquidity providers (LPs)** mettent des tokens en réserve et reçoivent des fees de trading proportionnellement à leur contribution à la liquidité de la pool, mais peuvent aussi faire des retraits.
3. **Les arbitrageurs** quand le prix proposé pour un trade permet un arbitrage.

Focus sur Uniswap 2/5

- Exemple : un LP apporte en liquidité 1 token A et 100 tokens B à un pool, soit 1% car les réserves suite à son apport sont de 100 tokens A et 10000 tokens B.
- Le LP pourra à tout moment retirer 1% de la réserve si elle n'évolue pas suite à d'autres apports, et **le LP ne maîtrise donc pas le nombre de tokens A et/ou B qu'il pourra retirer**.
- Supposons que le LP a apporté sa liquidité lorsqu'un token A valait 100 tokens B, le cours évolue et désormais un token A vaut 120 tokens B alors qu'il n'y a aucun apport de liquidité dans la pool entretemps. Imaginons qu'un arbitrageur prenne un trade tel que la réserve est désormais de $91{,}28$ tokens A et $10954{,}45$ tokens B (remarquant que $91{,}28 * 10954{,}45 \approx 100 * 10000$ et $10954{,}45/91{,}28 \approx 120$). Le LP peut donc retirer $0{,}9128$ tokens A et $109{,}5445$ tokens B, soit au cours actuel, en échangeant 9,5445 tokens B contre des tokens A, le LP peut désormais obtenir 0,9923 tokens A et 100 tokens B.
- Le LP a donc moins en portefeuille que s'il avait conservé le token A et les 100 tokens B initiaux sans jamais interagir avec l'AMM. On appelle cela **« l'impermanent loss »** (aussi appelée la divergence loss).
- Cette perte « disparaîtrait » si le cours revenait à 1 token A pour 100 tokens B et ne tient pas compte des frais perçus par le LP grâce aux trades de la pool.
- Un LP doit donc éviter les paires très volatiles avec un faible volume, en revanche les paires avec un comportement mean-reverting (typiquement les paires de stablecoins) sont potentiellement à privilégier, si le gain par les fees compense le coût d'opportunité de laisser du capital dans la pool.

Focus sur Uniswap 3/5

- La première version d'Uniswap impliquait d'utiliser des jetons d'ether (ETH) en guise de pont lorsqu'on souhaitait échanger un jeton ERC-20 contre un autre. Ainsi pour un échange désiré (exemple : convertir des DAI en USDT), il fallait absolument passer par ETH qui jouait le rôle de passerelle de conversion. Ce procédé rendait l'utilisation du système plus complexe et coûteux.
- La deuxième version d'Uniswap, sortie en mai 2020, a autorisé les échanges directs de jetons ERC-20.
- La troisième version d'Uniswap, implémentée en mai 2021, apporte la possibilité de concentrer sa liquidité sur une fourchette de prix particulière. Jusqu'à présent, celle-ci était répartie uniformément le long d'une courbe de prix, entre 0 et l'infini. Pour une grande majorité de pools, la majorité de la liquidité apportée n'était jamais utilisée. Avec Uniswap V3, les apporteurs de liquidité peuvent ainsi placer leur capital sur des fourchettes précises pour optimiser l'exploitation de leur liquidité et ainsi bénéficier de meilleures rémunérations. Ce système rapproche ainsi Uniswap d'un carnet d'ordres. Les frais uniques de 0,3% varient désormais entre 0,05%, 0,3% et 1% selon le type de paires (stablecoins, tokens très ou peu tradés).
- Aujourd'hui, Uniswapv2 et Uniswapv3 cohabitent.

Focus sur Uniswap 4/5

- Fin août 2020, SushiSwap a été déployé. Lancé par “Chef Nomi,” SushiSwap est un fork d’Uniswap.
- SushiSwap a proposé d’être un AMM géré par sa communauté à l’aide du token de gouvernance SUSHI. A ce moment-là, Uniswap ne proposait pas de gouvernance décentralisée.
- Les LPs de Sushiswap gagnent des tokens SUSHI en récompense lorsqu’ils apportent de la liquidité à un pool, ce qui n’était pas nouveau. Cependant, contrairement à Uniswap, les tokens SUSHI permettent aux détenteurs d’obtenir une portion des fees du protocole, qu’ils soient apporteurs de liquidité ou non. C’est une incitation pour les premiers utilisateurs à acquérir des tokens. SushiSwap a proposé 0.3% de frais de trading dont 0.25% aux LPs et 0.05% aux détenteurs de SUSHI.
- Pour prendre le contrôle des liquidités d’Uniswap, Sushiswap a proposé que des SUSHI puissent également être obtenus en stackant des tokens obtenus en étant LP sur Uniswap.
- Une migration considérable de liquidité d’Uniswap vers Sushiswap a suivi, pour ce qu’on appelle désormais une **“vampire attack”.**
- Une semaine après le lancement, la Total Value Locked (TVL) de Sushiswap a dépassé 1.5 milliard de dollars. En revanche, la TVL d’Uniswap a chuté de 1.8 milliards de dollars à 400 millions de dollars début septembre 2020.
- Cependant, un des cofondateurs de Sushiswap, Chef Nomi, a retiré des SUSHI sensés être dédiés au développement. Cela a entraîné une défiance et une brusque chute du cours du SUSHI.
- Chef Nomi a plus tard restitué les fonds. Mais la TVL de Sushiswap s’est effondrée, chutant de 1.5 milliard de dollars à 490 millions de dollars en environ une semaine.
- L’équipe d’Uniswap a lancé le token de gouvernance UNI dans la foulée. 400 UNI ont été distribués à toutes les adresses ayant interagi avec le protocole Uniswap avant le 1er septembre 2020.

Focus sur Uniswap 5/5

- Uniswap a émis un nombre maximal d'UNI jusqu'à 2024 dont 60% est donné aux utilisateurs, 21.5% aux employés et 18.5% pour les investisseurs. Avec 1 milliard d'UNI émis au "genesis block", la communauté a gagné les 60% qui lui revient en apportant de la liquidité.

- Pour les LPs, Uniswap a désigné **4 pools principales** pour gagner des UNI:

1. ETH/USDC

2. ETH/USDT

3. ETH/DAI

4. ETH/WBTC (wBTC, "wrapped BTC", projet lancé conjointement par plusieurs entreprises garantes dont BitGo et Kyber Network, est une représentation de BTC par un token ERC-20 sur la blockchain Ethereum)

- 1 milliard d'UNI n'est cependant pas le maximum. Après 2024, une inflation de 2% assure que les participants dans la gouvernance sont récompensés. Par le staking ou le vote, les utilisateurs obtiennent une part de l'inflation du protocole.

De nouveaux produits dérivés

- **Futures perpétuels dits “perps”** : Le perp est **un contrat futures qui n’a pas de maturité**, mais se base sur des “taux de financement” qui “alignent” le prix du perp avec le prix spot du sous-jacent. Introduit par BitMEX en 2016, les perps permettent de réduire la fragmentation de la liquidité des marchés de dérivés crypto en “concentrant” les différents marchés selon les dates de maturité en un seul. Les perps permettent aussi le “renouvellement” automatique d’un contrat sans payer de coûts de gas ou de renouvellement.
- **Options Atlantiques** : Pour un frais de transaction payé (souvent en stablecoins), les options atlantiques permettent à l’acheteur du put (resp. call) d’accéder au collateral de sa contrepartie et obtenir des revenus par staking, arbitrages etc. La clé est que le vendeur n’a (s’il n’y a pas d’erreur de design…) pas de risque de contrepartie : si le collateral est perdu par l’acheteur, il sera rémunéré à hauteur de ce qui a été perdu. La possibilité de retirer du collatéral permet de nombreuses stratégies pour les acheteurs d’options.