

Liquidity Baking

Raphaël Cauderlier

Nomadic Labs

April 27, 2021

Introduction

- Priorité numéro 1 du protocole
- Équipage
 - Bruno (DRI)
 - Sophia Gold (TQ)
 - Tom Jack (Marigold)
 - Zaynah
 - Boubacar
 - Arvid
 - Mehdi
 - Yann
 - moi

Historique

Été 2020	Développement de Dexter v1 (CamlCase) Vérification fonctionnelle de Dexter v1 (NL)
Octobre 2020	Lancement de Dexter v1 (CamlCase)
Décembre 2020	Liquidity Baking proposé sur Tezos Agora Sophia Gold (TQ) propose de l'implémenter
Février 2021	Arthur exige Liquidity Baking dans Florence Bug découvert dans Dexter, LB repoussé à Grenade Opération chevaliers blancs (NL et CamlCase) Lancement de Dexter v1.1 (CamlCase) Développement de Dexter v2 (Tom Jack)
Mars 2021	Vérification de Dexter v2 (NL)
Avril 2021	Intégration de LB dans le protocole (LB crew)
Futur proche	Vérification des propriétés économiques (NL)

Contrats de jeton

Smart contract avec:

- une table (adresse \rightarrow entier positif)
- une fonction de transfert

Contrats de jeton

Smart contract avec:

- une table (adresse \rightarrow entier positif)
- une fonction de transfert
- logique monétaire (comment les jetons sont créés ou détruits)

Contrats de jeton (Exemples)

- tzBTC
 - jetons convertibles avec les bitcoins
 - géré par Bitcoin Association Switzerland
 - supply: environ 360 BTC
- USDtz, ETHtez: meme principe, 300K\$ et 160ETH
- Kolibri: Stablecoin algorithmique 1,3M\$
- Governance tokens
 - jeton qui donne le droit de voter pour amender un projet

Échanges décentralisés (DEX)

Smart contract permettant d'échanger des jetons et des tez.

- Approche "Order book"
 - le smart-contract fait de la mise en relation entre acheteurs et vendeurs

Échanges décentralisés (DEX)

Smart contract permettant d'échanger des jetons et des tez.

- Approche "Order book"
 - le smart-contract fait de la mise en relation entre acheteurs et vendeurs
 - c'est lent

Échanges décentralisés (DEX)

Smart contract permettant d'échanger des jetons et des tez.

- Approche "Order book"
 - le smart-contract fait de la mise en relation entre acheteurs et vendeurs
 - c'est lent
 - en général trop lent pour des valeurs aussi volatiles
- Approche "Produit constant"
 - le smart-contract a la main sur des tez et des jetons (liquidités)
 - échange instantané
 - frais de change partagés entre les fournisseurs de liquidité

Constant Product Market Maker

Si on ignore les frais de change, chaque échange préserve l'invariant:

$$(A - dA) \times (B + dB) = A \times B$$

Avec:

- A: quantité de jetons sur le contrat
- B: quantité de tez sur le contrat
- dB: quantité de tez envoyés au contrat
- dA: quantité de jetons reçus du contrat

Constant Product Market Maker

Si on n'ignore pas les frais de change:

$$(A - dA - f) \times (B + dB) = A \times B$$

Avec:

- A: quantité de jetons sur le contrat
- B: quantité de tez sur le contrat
- dB: quantité de tez envoyés au contrat
- dA: quantité de jetons reçus du contrat
- $f = 0,3\%$ de dA

Incitatifs économiques

- Les fournisseurs de liquidités sont rémunérés proportionnellement au **volume** d'échange
- Pour un échange donné; moins il y a de volume, moins le taux de change est avantageux

Incitatifs économiques

- Les fournisseurs de liquidités sont rémunérés proportionnellement au **volume** d'échange
- Pour un échange donné; moins il y a de volume, moins le taux de change est avantageux
- problème de bootstrapping (aka. tragédie des communs)

Liquidity Baking

- Résolution du problème de bootstrapping par **création monétaire**:
 - chaque bloc contient une opération "Subsidy": 2.5tez ajoutés aux liquidités d'un Dex pour tzBTC
- Variante de Dexter v2:
 - pas de délégué
 - au lieu des 0,3% pour les fournisseurs de liquidité
 - 0,1% pour le fournisseurs de liquidité
 - 0,1% détruits
- Mécanismes d'arrêt
 - automatique après un niveau fixé d'avance (mais modifiable à chaque amendement)
 - arrêt d'urgence par un vote des bakers (un booléen par bloc, arrêt si une majorité des bakers des derniers bloc vote pour arrêter)

- Majorité du code mergée ce matin
- Réseau de test lancé très bientôt
- Pas encore actif si activé sur mainnet
- Preuves en cours