OAK INVEST

Oracles Web3 : Une révolution invisible.

SPONSORISÉ PAR PYTH

R 20000 - 001 - F: 0,00 €

SOMMAIRE

TLDR	3
Préface Introduction Présentation Oak Présentation Pyth Network	4
Comprendre les oracles Comment les oracles fonctionnent Qu'est ce qu'un oracle Briser les barrières de la blockchain Les différents types d'oracles La structure utilisée Oracles Inbound vs Outbound Oracles Centralisés vs Décentralisés Oracles Software vs Hardware Les protocoles sans oracle	9
Le paysage actuel des oracles Introduction de la TVS La place des oracles dans la DeFi Les Data Providers VRF Identity Oracles de crédit Une place importante dans les NFTs Chainlink : un monopole incontesté jusqu'à présent	20
Les tokens d'oracles À quoi servent les tokens d'oracles Financement du projet Moyen de paiement Incentive à fournir des données fiables La gouvernance Exemples d'utilisation Intéressant pour les particuliers ? Les risques liés aux tokens d'oracles	32

SOMMAIRE

Les défis et challenges des Oracles — 39
- Les vecteurs de vulnérabilité
  - Manipulation de prix
  - L'infrastructure off-chain
  - La confiance en une entité
  - Les risques de la décentralisation
  - Freeloading
  - Mirroring
- Les bugs et les hacks
  - "It's not a bug, it's a feature"
  - L'implémentation d'un oracle
  - Les flash loans

La réglementation des oracles — 44
- En Europe
  - L'approche des régulateurs français
  - Les pistes de réglementation
- Aux États-Unis

Les perspectives — 51
- L'avenir des oracles
- L'intégration des oracles dans l'IA et l'IOT
- L'émergence des casinos Web 3
- Le mot de la fin

Remerciements — 57

Disclaimer — 58

Lexique — 59

TLDR

Les oracles jouent un rôle crucial dans l'écosystème. En effet, **ils permettent à la blockchain d'interagir avec des données et des événements du monde réel.**

Les oracles sont les ponts qui connectent ces deux mondes entre eux.

Ces derniers peuvent être classés selon plusieurs critères : la direction du transfert d'information (Inbound vs Outbound), le niveau de centralisation (Centralisés vs Décentralisés), le type (Software vs Hardware) et bien d'autres...

Bien qu'actuellement **les oracles jouent un rôle déterminant dans le secteur de la finance décentralisée (DeFi),** ces derniers ont diversifié leurs applications vers l'identification, les jeux de hasard, les NFTs ou encore la vérification de crédit.

En parallèle, **les tokens d'oracle** ont émergé comme un outil pour financer les projets d'oracle, servir de moyen de paiement, inciter à fournir des données précises, et faciliter la gouvernance au sein de ces systèmes. **Ces derniers sont aujourd'hui capitalisés à plusieurs milliards de dollars.**

Les oracles font face à de nombreux défis. Ils sont sujets à diverses vulnérabilités, incluant la manipulation des prix, les risques associés à la décentralisation, et les attaques par flash loans.

De plus, les régulateurs commencent à s'intéresser à leur encadrement tant en Europe qu'aux États-Unis.

En regardant vers l'avenir, les oracles ont le potentiel de transformer non seulement l'écosystème de la blockchain, mais aussi le monde plus traditionnel que nous connaissons tous.

Leur capacité à fournir des données fiables et sécurisées en temps réel ouvrira sans doute la porte à de nouvelles innovations.

INTRODUCTION

L'homme a toujours cherché à comprendre les messages et les volontés des divinités. Dans la mythologie grecque, l'oracle était un intermédiaire sacré, une passerelle entre les dieux et les hommes, délivrant prophéties et conseils divins.

Aujourd'hui, dans l'univers numérique de la blockchain, les oracles jouent un rôle similaire mais d'une nature différente. Ces derniers servent de **pont entre le monde décentralisé et numérique de la blockchain et le monde réel**, dense, dynamique et rempli d'informations et de données.

La blockchain, de par son potentiel révolutionnaire de décentralisation et de sécurisation des transactions, se heurte néanmoins à une limitation cruciale : son incapacité intrinsèque à **accéder directement aux données du monde réel**. Pour déployer pleinement son potentiel et son utilité, elle doit être capable d'interagir avec un éventail de données réelles, comme le cours de bourse ou les résultats de matchs sportifs par exemple.

Dans ce contexte, les oracles blockchain endossent le rôle crucial d'intermédiaires en **récupérant et intégrant les données externes à la blockchain** pour permettre l'exécution de smart contracts.

Lors de l'émergence de la blockchain, l'absence de normes et de leaders établis a donné naissance à un véritable "Far West", chaque protocole cherchant à élaborer son propre oracle pour établir une connexion avec le monde réel.

Cependant, la conception d'une telle solution s'est avérée être un défi de taille. De nombreux oracles “faits maison” se sont révélés inefficaces et vulnérables, aboutissant à d'importants piratages et à la perte ou au vol de plusieurs millions de dollars.

Face à cette problématique, de nouveaux oracles plus adaptés ont fait peu à peu leur apparition dans le paysage blockchain. Chacun de ces acteurs, avec **ses spécificités techniques et ses mécanismes de sécurité propres**, cherche à apporter une réponse aux lacunes observées.

Avec le temps, les oracles ont progressivement renforcé leur présence, devenant des éléments indispensables pour l’écosystème.

Les oracles **évoluent de pair** avec l’environnement crypto en suivant de près ses tendances, à la hausse comme à la baisse. Cette relation indissociable fait que les oracles reflètent non seulement les innovations mais aussi les fluctuations du marché. Leur développement et leur performance sont directement influencés par les mouvements et les dynamiques de ce secteur en constante évolution.

Au moment de l’écriture de ces lignes (09/23) :

$1050	$37.5
Capitalisation totale des cryptomonnaies (Milliards)	**TVL de la Finance Décentralisée (Milliards)**

Ce dossier propose une exploration approfondie de l'univers des oracles blockchain.
Un lexique est à votre disposition à la fin de ce dossier pour faciliter la compréhension des termes employés.
Bonne lecture !

PRESENTATION OAK INVEST

OAK Invest est un média indépendant spécialisé dans le domaine de l'investissement proposant du contenu informatif avec une approche innovante et dynamique sur les réseaux sociaux. Notre objectif est de rassembler une communauté d'investisseurs de tous niveaux en quête de connaissances claires et accessibles.

Nous mettons également notre expertise du digital à la disposition des professionnels de la finance pour les aider à gagner en visibilité, crédibilité et efficacité à travers notre agence Wasabee Consulting.

@oak_fr @oak.invest OAK Invest OAK Invest

Nous contacter :

Contact média : contact@oakinvest.fr
Contact agence : contact@wasabee-consulting.com

WASABEE

PRESENTATION PYTH NETWORK

Pyth Network est une solution d'oracle qui vise à résoudre un problème crucial dans l'écosystème de la finance décentralisée (DeFi) : la latence et l'inexactitude des données financières.

Lorsqu'il s'agit de blockchain et de smart contracts, il est essentiel d'avoir accès à des informations financières précises et disponibles en temps réel. Cependant, en raison de la nature décentralisée de ces systèmes, les données peuvent souvent être retardées ou inexactes et peuvent ainsi entraîner des conséquences graves.

PYTH

Pyth Network a développé un oracle qui dispose d'une supériorité technique à toute épreuve avec une solution à ces problèmes en fournissant des données financières précises et instantanées directement aux utilisateurs ainsi qu'aux applications décentralisées (DApps).

Le réseau Pyth utilise une méthode appelée "Price Aggregation" pour garantir la précision des données. Contrairement à d'autres oracles qui rassemblent simplement des données à partir de sources gratuites sur Internet, Pyth combine des informations à la fois on-chain (sur la blockchain) et off-chain (en dehors de la blockchain).

L'oracle utilise un algorithme d'arbitrage pour comparer les données de plusieurs "fournisseurs" avant de déterminer une valeur unique qui est ensuite transmise aux "consommateurs" de données. Cela permet de garantir des informations aussi précises que possible.

Initialement lancé sur le réseau Solana, Pyth a depuis évolué pour devenir une solution indépendante.

Les services de Pyth Network bénéficient de partenaires reconnus pour assurer l'approvisionnement en données fiables tel que Amber Group, BitBank, Bitstamp, CoinShares, Kaiko, Gate.io, Gemini Exchange, Huobi, Jump Trading, Kucoin, MEXC, Talos pour en nommer quelques-uns.

Vous pouvez retrouvez la liste des fournisseurs de données ici :
https://pyth.network/publishers

Voici quelques chiffres sur cet oracle prometteur :

+80
Data Providers

+280
Feeds de données

>30
Blockchains

$50B
De volume de trading

Pyth Network est une innovation majeure dans le domaine de la DeFi, offrant une solution robuste et fiable pour le problème persistant de la latence et de l'inexactitude des données financières. Avec son approche technique avancée et son écosystème bien conçu, Pyth est bien positionné pour devenir un acteur clé majeur dans le développement d'un écosystème DeFi plus sûr, plus précis et plus efficace.

@PythNetwork

pyth.network

Le 28 Septembre, Pyth Network ont publié leur Whitepaper 2.0 annonçant le lancement de leur token.

Ce dernier servira à décentraliser la gouvernance du protocole mais sera aussi utilisé comme garant pour les différents fournisseurs de données.

Dans ce document, l'oracle entre en détail sur la façon dont leur vision et technologie ont évoluées depuis leur conception.

En savoir plus sur le Whitepaper

Vous pouvez y accéder directement via ce lien.

DEONTOLOGIE DE REDACTION

Avant de plonger dans le cœur de ce dossier de recherche, il est important de souligner l'engagement de notre média envers l'indépendance éditoriale et la déontologie appliquée pendant la rédaction de ce dernier.

Bien que cette enquête ait été réalisée avec le soutien de Pyth Network, nous tenons à assurer à tous les lecteurs que le contenu demeure entièrement indépendant et exempt de toute influence extérieure.

Les données présentées, les analyses effectuées et les conclusions tirées sont le fruit d'un travail rigoureux basé sur des faits ainsi que des sources présentes en fin du dossier. Notre sponsor n'a eu aucun droit de regard sur le contenu, la méthodologie ou les conclusions de celui-ci.

Notre objectif demeure, comme toujours, de fournir une information fiable, objective et pertinente à notre audience. La confiance que vous avez accordée à nos précédentes recherches nous est précieuse et nous nous engageons à maintenir les plus hauts standards éthiques et professionnels.

La Sibylle de Cumes d'Andrea del Castagno (1419-1457)

COMPRENDRE LES ORACLES

Avant toute chose, il est essentiel de poser les bases et de définir clairement ce qu'est un oracle. La première partie de ce dossier se consacre entièrement à cette notion, afin de démystifier son fonctionnement et mettre en lumière son rôle majeur dans le paysage actuel.

COMMENT FONCTIONNENT LES ORACLES ?

Qu'est ce qu'un oracle ?

En raison de sa nature décentralisée et sécurisée, une blockchain ne peut, par conception, accéder directement à des informations extérieures, bien que de nombreuses applications en aient besoin pour fonctionner. Par exemple, le prix en temps réel d'un produit financier ou tout simplement des données météorologiques.

Le rôle des oracles est de fournir à la blockchain des données extérieures de manière fiable et sécurisée.

Ainsi, un oracle blockchain agit comme un intermédiaire, fournissant des données externes à la blockchain et lui permettant d'interagir avec le monde extérieur.

Voici un exemple concret pour mieux comprendre leur utilisation :

Deux amis décident de faire un pari basé sur le résultat du match Paris SG / FC Metz.
Si Paris gagne, l'ami A doit 5 € à l'ami B. Dans le cas contraire, l'ami B doit 5 € à l'ami A.

Pour automatiser ce processus, ils décident d'utiliser un smart contract sur une blockchain. (Notons que ces deux amis aiment beaucoup la tech.)

Ils programment alors ce smart contract capable d'accepter les mises, de les stocker et de transférer l'ensemble des fonds au gagnant une fois le match terminé.

Les deux amis envoient 5 € au smart contract. En l'état actuel, le smart contract est un programme enfermé dans une boîte noire : il ne peut pas connaître le résultat du match et ne peut donc pas distribuer les fonds au gagnant.

C'est ici qu'intervient l'oracle, l'intermédiaire nécessaire pour obtenir cette information !

Comme mentionné, l'oracle recueille les informations du monde extérieur pour les introduire sur la blockchain. Dans cet exemple, l'oracle serait configuré pour interroger des sites de résultats sportifs à la fin du match, les récupérer, puis envoyer le score final au smart contrat.

Suite à cela, le smart contract déterminera lequel des deux amis est le gagnant, en fonction du résultat transmis, et distribuera les fonds en conséquence.

Si Paris a gagné, le smart contract envoie automatiquement 10 € (mise + gain) à l'ami B. Si Paris a perdu, il envoie automatiquement les fonds à l'ami A.

On comprend ici la métaphore souvent utilisée qui définit les oracles comme des ponts reliant les fournisseurs de données hors chaîne aux smart contract sur les blockchains.

Briser les barrières de la blockchain

Un smart contract est un programme informatique qui s'exécute de manière autonome et qui facilite la mise en œuvre d'accords entre différentes parties dès lors que certaines conditions prédéfinies sont atteintes, d'où l'appellation « smart contracts » ou « contrats intelligents ».

Bien qu'ils soient qualifiés d'"*intelligents*", ils sont, dans la plupart des cas, déterministes par nature.

Un smart contract est souvent dit "déterministe" car il produira **le même état final à partir d'un état initial donné** et d'une série de transactions.

Autrement dit, chaque fois que vous procédez à une transaction sur la blockchain à partir d'un état donné, vous obtiendrez toujours le même résultat. Bien que cela puisse paraître logique, il est crucial que cette propriété soit maintenue pour **garantir la cohérence et la fiabilité des données** sur la blockchain.

Imaginons une sonnette de porte. À chaque pression, elle émet un signal sonore signalant une visite. C'est un système déterministe : quel que soit le moment ou la force d'appui, le son est toujours le même, sans exception.

On peut faire le parallèle avec une sonnette en mauvais état qui ne fonctionne pas à tous les coups. Ce système serait dans ce cas non-déterministe, comme le lancer d'un dé : malgré des conditions initiales quasi-identiques, le résultat est imprévisible et peut varier à chaque essai.

Le fonctionnement des blockchains repose sur la capacité des nœuds à atteindre un consensus, une majorité de même choix, sur des questions binaires, comme "vrai" ou "faux", en se fondant uniquement sur les informations présentes sur la blockchain.

Voici comment cela se traduit dans des exemples concrets :

- La transaction a-t-elle été signée par le bon propriétaire du compte ? Vrai / Faux ?
- Y a-t-il assez de fonds dans le compte pour effectuer cette transaction ? Vrai / Faux ?
- Cette transaction est-elle conforme aux règles du contrat intelligent concerné ? Vrai / Faux ?

Le déterminisme est essentiel pour assurer que tous les nœuds arrivent à la même conclusion. Si différents nœuds obtiennent des résultats divergents, cela brise le consensus et compromet la fiabilité d'une blockchain en tant que système décentralisé.

Les oracles jouent un rôle clé en introduisant des données externes dans la blockchain, tout en préservant cette propriété déterministe essentielle.

En collectant et en intégrant des informations de sources extérieures à la blockchain pour qu'elles soient utilisées par des smart contracts, **on assure l'inaltérabilité et l'accessibilité universelle de ces données.**

De cette façon, les nœuds d'une blockchain peuvent s'appuyer en toute confiance sur les données transmises par l'oracle sans menacer le consensus.

Les différents types d'oracles

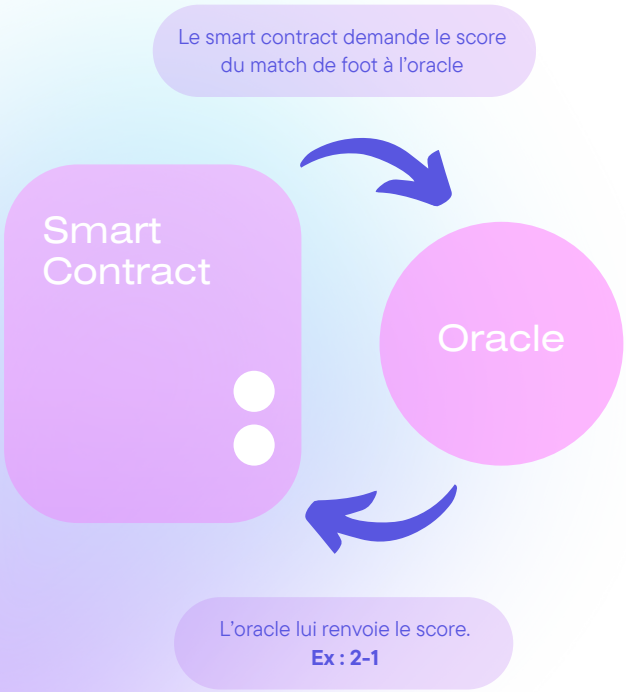
Les oracles peuvent être classifiés en fonction de plusieurs critères :

- l'origine des informations qu'ils collectent (unique ou multiple)
- le type de système de confiance sur lequel ils s'appuient (centralisé ou décentralisé)
- la structure du système qu'ils utilisent (qu'il s'agisse d'une récupération directe de données, d'un système de publication et d'abonnement, ou d'un format de demande et de réponse)

De plus, on distingue les oracles sur la base des fonctions qu'ils remplissent : certains collectent des données off-chain (en dehors de la blockchain) pour les utiliser dans les contrats on-chain (sur la blockchain), d'autres transmettent des informations de la blockchain vers des applications off-chain ou on-chain.

La structure utilisée

Immediate-read

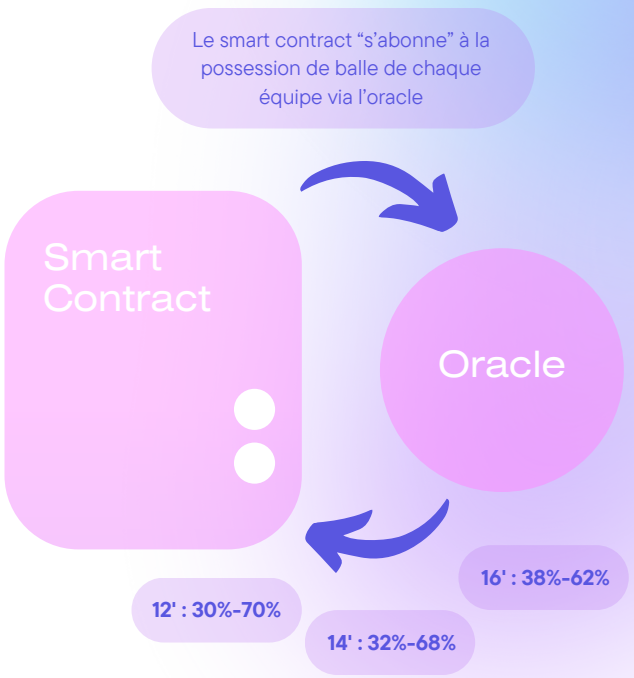


Les oracles fournissent des données primordiales afin de prendre des décisions immédiates. “Cette personne a-t-elle voté aux dernières élections ?" Ce type de données est généralement sollicité à la demande, c'est-à-dire exactement au moment où l'information est nécessaire.

Les oracles introduisant des données destinées à des prises de décision rapides conservent ces informations dans le stockage associé au smart contract. Ces données sont par ailleurs régulièrement mises à jour.

Dans l'exemple précédent concernant le pari sur le résultat du match PSG - FC Metz, un tel oracle serait parfaitement adapté. La donnée n'est nécessaire qu'une seule fois, à l'issue du match et n'a pas besoin d'être actualisée périodiquement.

Publish-subscribe

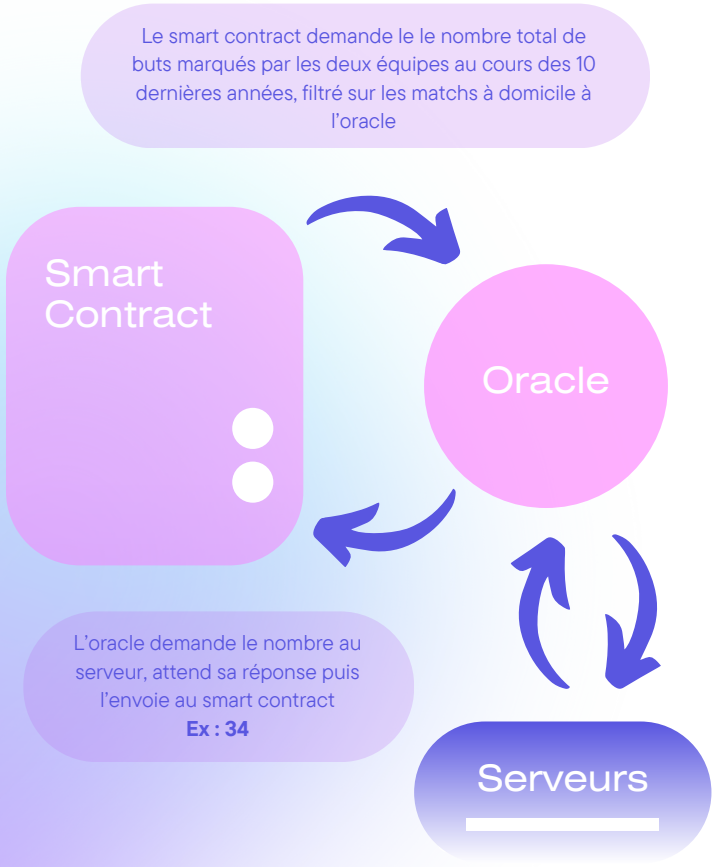


Dans ce scénario, l'oracle sert principalement de canal de diffusion pour des informations susceptibles de subir des modifications, que cela soit de manière régulière ou occasionnelle. Les données seront transmises au smart contract à la demande de ce dernier ou par l'intermédiaire d'un agent off-chain surveillant les mises à jour de l'oracle.

Reprenons l'exemple du pari sur le match de foot : nos deux amis pourraient miser sur la possession de balle sur les 5 prochaines minutes. Ils auront donc besoin de recevoir, à des intervalles irréguliers, des mises à jour sur cette statistique.

Ces oracles sont particulièrement prisés en Finance Décentralisée car les prix doivent être constamment actualisés pour déterminer la valeur de chaque cryptomonnaie lors des échanges, des liquidations et de toutes autres opérations financières sur la blockchain.

Request-response



Ce modèle est semblable à l'architecture client-serveur dans laquelle une demande est envoyée par le client et traitée par le serveur.

Les données de cet oracle pourraient être conservées dans une infrastructure externe car elles proviennent d'un ensemble de données trop volumineuses pour être stockées dans le smart contract. Du fait de ce contexte et de la nécessité de performances accrues, ces types d'oracles exploitent une infrastructure hors chaîne, tels que des serveurs.

Dans notre exemple, les deux amis pourraient miser sur le nombre total de buts marqués par les deux équipes au cours des 10 dernières années, filtré sur les matchs à domicile.

Inbound ou Outbound Oracles ?

Les oracles facilitent la circulation d'informations entre les blockchains et l'extérieur. Selon le sens de cette circulation, on distingue principalement deux types d'oracles : **"inbound" pour les données entrantes et "outbound" pour les données sortantes.**

Oracles Inbound

Les oracles "inbound" facilitent la circulation des données entrantes, c'est-à-dire qu'ils acheminent des informations du monde extérieur vers la blockchain. C'est le modèle le plus connu et cité jusqu'ici dans ce dossier.

Oracles Outbound

À l'opposé, les oracles "outbound" gèrent la circulation des données sortantes. Ils prennent des informations de la blockchain et les transmettent à des entités extérieures.

Imaginez vouloir que votre système domotique à domicile joue une chanson de victoire à chaque fois que le prix du Bitcoin dépasse son ATH. Vous pouvez mettre en place un smart contract qui surveille le prix de la cryptomonnaie en envoyant une commande à votre système domotique grâce à l'utilisation d'un oracle sortant.

Centralisation ou décentralisation ?

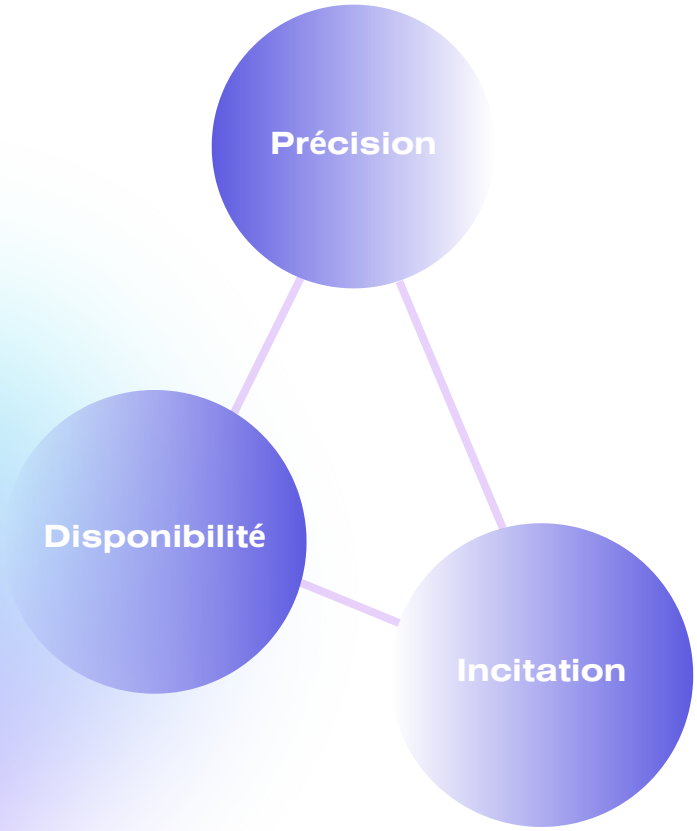
Le trilemme des oracles

Vous êtes probablement déjà familier avec le trilemme des blockchains et celui des stablecoins. Abordons ici le trilemme des oracles.

Jouons à un jeu et tentons de découvrir le meilleur oracle du monde.

Dans un monde idéal, un oracle serait techniquement en mesure d'inciter les fournisseurs de données hors chaîne à soumettre des informations exactes et rapides puis de les distribuer aux utilisateurs finaux (protocoles) tout en étant disponible 24h/24 et 7j/7.

Bien que cette description semble simple, les équipes en charge des oracles travaillent d'arrache pied pour obtenir un tel résultat.



- **Précision des données :** Un oracle doit s'assurer que les informations fournies soient fiables et n'aient pas été altérées pour que les smart contracts ne fassent pas d'erreurs basées sur de fausses données.

- **Disponibilité :** Un oracle doit toujours être prêt à fournir des informations aux smart contracts pour qu'ils puissent faire leur travail sans interruption. Il ne doit pas y avoir de délais ou d'obstacles qui empêchent les smart contracts de prendre des décisions ou d'agir. Les informations doivent être là quand on en a besoin, en permanence.

- **Compatibilité incitative :** La compatibilité incitative implique l'attribuabilité et la responsabilité. L'attribuabilité permet de corréler une information externe à son fournisseur, tandis que la responsabilité lie les fournisseurs de données aux informations qu'ils donnent, de sorte qu'ils puissent être récompensés ou pénalisés en fonction de la qualité des informations fournies.

Ce trilemme peut également s'étendre au degré de décentralisation, au coût de l'oracle, à la diversité des fournisseurs et à d'autres critères que chacun pourrait juger plus ou moins importants, illustrant ainsi les compromis que les oracles pourraient être amenés à faire dans leurs choix de conception.

À l'image de la majorité des entreprises web3, les oracles peuvent être classifiés en deux catégories : les oracles centralisés et les oracles décentralisés.

Il est essentiel de comprendre les différences entre ces deux types d'oracles.

Afin d'y voir plus clair, explorons ces deux modèles à travers le trilemme mentionné précédemment.

Les oracles centralisés

Un oracle centralisé est géré par une unique entité ou personne.

Ce type d'oracle est réputé pour sa rapidité et son efficacité car il n'existe qu'une seule source distribuant les informations. Cela peut s'avérer avantageux, particulièrement lorsque les informations émanent directement d'une source reconnue comme fiable.

Revisitons le trilemme évoqué précédemment pour examiner comment les oracles centralisés satisfont chacun des trois critères :

- **Précision des données :**

Pour : Un oracle centralisé peut garantir une meilleure précision des données car il peut directement contrôler et valider la source mais aussi l'intégrité des données avant de les transmettre au smart contract. Puisqu'il est l'unique preneur de décisions, il ne peut y avoir de désaccord au niveau des fournisseurs de données.
Contre : Si l'oracle centralisé est compromis ou malveillant, il peut délibérément fournir des données inexactes, et étant la seule source de données, il n'y a pas de mécanisme de vérification ou de correction. Ainsi, l'oracle représente l'unique point de défaillance de par sa nature centralisée.

- **Disponibilité :**

Pour : La gestion centralisée des ressources peut garantir une haute disponibilité et un temps de réponse rapide pour les smart contracts.
Contre : Étant un point unique de défaillance, si un oracle centralisé rencontre un problème technique ou est attaqué, la disponibilité des données peut être interrompue.

- **Compatibilité incitative :**

Contre : Les oracles centralisés présentent souvent des mécanismes d'incitation mal conçus, voire inexistants, afin de garantir que le fournisseur de données transmette des informations fiables et non modifiées. L'un des points de vigilance majeurs est la renommée du fournisseur de données. Bien que les projets préfèrent adopter un oracle décentralisé, la réputation de l'acteur centralisé peut souvent jouer en sa faveur. Une fois cette réputation rompue, l'oracle peut perdre des clients du jour au lendemain.

Les oracles décentralisés

Les oracles décentralisés sont des systèmes dans lesquels plusieurs participants collaborent pour fournir des informations fiables.

Contrairement à leurs homologues centralisés, les oracles décentralisés puisent leurs données de plusieurs sources différentes qui ne communiquent pas entre elles. Afin de consolider toutes ces informations, un consensus est mis en œuvre par l'oracle pour transmettre une donnée unifiée au protocole avec lequel il interagit.

Examinons comment ils répondent au trilemme des oracles :

- **Précision des données :**

Pour : Avec plusieurs sources de données, un oracle décentralisé peut agréger l'information, obtenir un prix médian entre tous les fournisseurs de données et transmettre la donnée valide. Les acteurs tentant de corrompre le réseau avec de fausses informations sont financièrement sanctionnés, réduisant ainsi le risque d'attaque.

De plus, corrompre une multitude de sources s'avère plus compliqué qu'une unique source centralisée.
Contre : La diversité des sources peut conduire à des désaccords et de l'incertitude concernant la précision des données. Cela explique l'importance d'établir un consensus efficace tout en diversifiant les sources afin d'assurer le bon fonctionnement de l'oracle décentralisé.

- **Disponibilité :**

Pour : La nature distribuée des oracles décentralisés accroît la résilience et minimise le risque de panne totale car la défaillance d'un fournisseur n'affecte pas la disponibilité des autres.
Contre : La coordination entre les différents nœuds et fournisseurs d'informations peut occasionner de la latence et altérer la disponibilité des réponses.

- **Compatibilité incitative :**

Pour : La diversité des participants peut conduire à une concurrence saine et à un renforcement des incitations à fournir des données plus précises et plus fiables.

Compte tenu des enjeux et des préoccupations relatives à la gestion du risque de confiance, de nombreuses applications DeFi privilégient les oracles décentralisés au détriment de ceux centralisés pour transmettre des données sur la blockchain.

Le débat se porte néanmoins sur **le degré réel de décentralisation des oracles.** Selon les standards de l'industrie et les perspectives individuelles, un oracle peut être considéré comme tel ou non. Ainsi, comme avec les blockchains, nous parlerons plutôt de degrés de décentralisation, qui varient selon de nombreux paramètres."

Software ou Hardware Oracles ?

Bien que poursuivant des objectifs similaires, les oracles de blockchain emploient des méthodes diverses de "sourcing" en raison de la multitude de données disponibles dans le monde réel. On différencie notamment les Software Oracles et les Hardware Oracles.

Les Software Oracles

Un Software Oracle sert de liaison entre Internet et la blockchain. Il collecte des données depuis diverses sources en ligne, telles que les bases de données, les interfaces d'API (Application Programming Interface), les réseaux sociaux ou encore les serveurs, avant de les transmettre à la blockchain.

En raison de leur adaptabilité et de la variété des informations qu'ils peuvent traiter, dont les données financières, les Software Oracles sont naturellement les plus utilisés.

Ils jouent un rôle crucial en fournissant aux smart contracts des informations à jour comme les données relatives aux prix des actifs numériques.

Prenons un exemple concret :

Imaginons un smart contract sur une blockchain qui permet aux utilisateurs d'acheter ou de vendre une option sur une entreprise spécifique, disons "OakLtd".

Pour le bon fonctionnement de ce contrat, il doit connaître le prix du "OakLtd" à tout moment.

Sources de données : l'oracle est configuré pour se connecter à trois plateformes d'échange. Ces plateformes offrent des API permettant d'accéder aux prix en temps réel des entreprises cotées, dont "OakLtd".

Collecte de données : Toutes les 10 secondes, l'oracle interroge ces trois plateformes pour obtenir le prix de "OakLtd".

Traitement des données : Une fois les données collectées, l'oracle calcule une médiane des trois prix afin de minimiser les risques d'erreurs ou de manipulations sur une plateforme spécifique. À noter que cet exemple est simplifié et que la calibration des données sur les oracles dits “traditionnels” est très complexe.
(https://pyth.network/blog/pyth-price-aggregation-proposal)

Transmission à la blockchain : Après avoir calculé la médiane, l'oracle transmet cette information au smart contract sur la blockchain.

Smart contract : Le smart contract reçoit le prix de "OakLtd" et l'utilise pour évaluer l'option, déclencher des ordres d’achat ou de vente ou réaliser toute autre action prévue dans le contrat en fonction de la donnée fournie par l’oracle.

Les Hardware Oracles

Un oracle hardware, quant à lui, fait appel à des dispositifs matériels tels que des capteurs électroniques pour recueillir des informations du monde réel. Ces données sont ensuite converties en valeurs numériques, rendant ainsi possible leur lecture et utilisation par des smart contracts.

Ces oracles matériels sont particulièrement robustes et résistants.

Ils sont essentiels dans diverses applications telles que la gestion des chaînes d'approvisionnement, la localisation pour les services de livraison ou encore la collecte de données météorologiques. Il est également important de noter qu’il est bien plus compliqué de corrompre ou modifier les données d’une pièce de hardware qu’une donnée numérique.

Reprenons un exemple concret en utilisant la même base pour comprendre la différence :

Vous avez une entreprise de transports de marchandises surgelées pour lesquelles la chaîne de froid ne doit en aucun cas être interrompue. Actuellement, les données des compteurs installés dans les camions sont relevées par vos employés à la fin de chaque livraison.

Jugeant ce système peu efficace, vous décidez de retirer votre confiance en la gestion humaine. Vous connectez donc vos capteurs de température situés à l’intérieur des camions à un smart contract. En cas d'augmentation de température celui-ci enregistre un message d'alerte sur la blockchain indiquant que les produits ne sont plus consommables.

Pour mettre en œuvre ce dispositif :

- Installez de nouveaux capteurs de température dans les camions. Ces capteurs, étant inviolables, intègrent un système de protection s’activant si une tentative de déplacement par vos employés est détectée.

- Toutes les 10 minutes, ce capteur transmet la température relevée à l’oracle.

- L’oracle collecte cette information. Si la température est conforme aux standards, aucune action n'est déclenchée. En cas de variation de la température, le smart contract active une alerte, qui est ensuite enregistrée sur la blockchain.

À l’arrivée du camion, le récepteur peut simplement consulter la blockchain pour vérifier si des alertes ont été émises pendant le trajet.

BONUS : Vous avez également la possibilité de mettre en avant votre service irréprochable en offrant aux consommateurs la possibilité de consulter ces mêmes données, vous permettant ainsi de vous prémunir contre d'éventuels litiges.

PROTOCOLES SANS ORACLE

On peut légitimement se demander s’il est possible pour un protocole de se passer d’un oracle pour fonctionner.

Spoiler : c’est possible, dans certains cas.

Des avancées récentes ont été réalisées pour répondre aux préoccupations liées aux oracles, en particulier en matière de décentralisation, de transparence et de vérifiabilité des données.

Il existe des protocoles, **dits "oracle-less"**, qui utilisent des mécanismes alternatifs pour obtenir des résultats similaires aux protocoles fonctionnant avec des oracles. Ces protocoles offrent des avantages tels que la protection contre la manipulation des prix liée aux oracles, une sécurité accrue en réduisant les vulnérabilités externes et des économies de coûts en évitant les frais d'oracle.

Voici quelques exemples pour comprendre comment ces protocoles fonctionnent et quels sont leurs avantages et inconvénients.

PWN Finance

PWN Finance est une plateforme de prêt peer-to-peer sans oracle.
Au lieu de s'appuyer sur des flux de prix externes, PWN facilite les correspondances directes entre emprunteurs et prêteurs, leur permettant d'établir leurs propres conditions de crédit.

Les emprunteurs listent les détails souhaités de leur prêt et leur collatéral tandis que les prêteurs présentent leurs conditions de crédit.

Une fois que deux parties se trouvent et sont d'accord, l'emprunteur reçoit le prêt et le prêteur obtient un “deed token” qui leur donne le droit de réclamer le collatéral en cas de défaut.

Lorsque les prêts arrivent à échéance, les emprunteurs peuvent rembourser la somme initiale accompagnée des intérêts convenus à l’avance. En cas de défaut, les prêteurs peuvent réclamer le collatéral.

Les fluctuations de la valeur du collatéral pendant la durée du prêt n'ont pas d'impact sur l'emprunteur et ne provoquent pas une liquidation soudaine sur ce type de protocole.

Les points forts **du modèle de PWN Finance résident dans sa simplicité**, éliminant le besoin d'oracles ou de Lending Pools. Comme les conditions de prêt sont convenues à l'avance, la valeur du collatéral n'influencera en rien la position de l'emprunteur au cours du prêt.

Ce modèle présente cependant des risques pour les prêteurs.
Si la valeur du collatéral chute en dessous du montant du prêt à la fin du terme, les emprunteurs pourraient être incités à faire défaut et à abandonner leur collatéral maintenant dévalué.

Les prêteurs pourraient alors se retrouver dans des situations où ils recevraient un collatéral qui vaut moins que le prêt qu'ils ont accordé.

Le prêt sans oracle donne **la possibilité aux prêteurs de définir eux-mêmes** la valeur des garanties et les critères liés au risque. Cela signifie que la responsabilité de suivre les prix, d'évaluer les risques et de prendre des décisions concernant les liquidations est déplacée vers une approche de pair à pair.

Blend

Blend est un projet de la marketplace de NFT Blur (Blur + Lending = Blend) qui permet aux utilisateurs d'emprunter en utilisant un NFT en tant que collatéral, le tout sans oracle.

Blend se confronte à différents défis :

- Comment définir sa capacité d'emprunt à partir d'un NFT ? Se baser sur le floor de la collection ou alors sur les offres d'achat ?
- Comment évaluer la valeur réelle d'un NFT ?

Sur Blend, les prêteurs déterminent les conditions de prêts qu'ils souhaitent (le montant maximal du prêt, le taux d'intérêt et les collections de NFTs qui leur conviennent en tant que collatéral).

Une fois qu'un accord avec un emprunteur est conclu, le NFT servant de garantie détenu par l'emprunteur est verrouillé dans un smart contract et les fonds prêtés lui sont délivrés.

La spécificité de Blend se retrouve dans sa structure sans oracle, obtenue en employant un mécanisme de vente aux enchères hollandaise pour la liquidation des prêts.

Si le prêteur veut récupérer son argent au cours du prêt, le prêteur peut engager un processus spécifique à la plateforme :

- Ce dernier initie une enchère hollandaise pour trouver un nouveau prêteur. Les taux du prêt commencent à 0% et continuent d'augmenter jusqu'à un certain niveau.
- Si une personne veut reprendre cette dette, elle devra rembourser le prêteur et deviendra à son tour créancier de l'emprunteur.
- Si personne ne reprend cette dette, le NFT déposé en collatéral est envoyé au prêteur.

L'adjudication **à la hollandaise** est une technique de vente au cours de laquelle un bien est mis aux enchères à un prix plus élevé que sa valeur et dont le prix est progressivement abaissé jusqu'à ce qu'il trouve acheteur.

Dernièrement, Blend a constaté une augmentation notable du nombre de plateformes de prêt et d'emprunt de NFT. La plateforme conserve cependant une position dominante avec environ 80% du volume total du secteur.

L'inconvénient de ce modèle repose sur le transfert des responsabilités en matière d'évaluation des risques. Contracter de tels prêts nécessitent des compétences et du temps pour surveiller les prix du marché.

Si vous souhaitez en savoir plus sur les protocoles oracle-less, nous vous invitons à lire le rapport récent de Binance Research à ce sujet.

LE PAYSAGE ACTUEL

Après avoir exploré la nature et le fonctionnement des oracles dans l'écosystème, il est impératif de se pencher sur le paysage actuel. **Les oracles évoluent dans un environnement complexe et diversifié, façonné par les exigences variées des applications décentralisées et les innovations continues**.

INTRODUCTION DE LA TVS

Dans le monde de la blockchain, il est possible d'évaluer la croissance et l'adoption avec plusieurs métriques bien connues.

L'une des mesures les plus populaires est la Total Value Locked (TVL), qui représente la valeur totale des actifs déposés dans les protocoles de la Finance Décentralisée (DeFi).

Puisque les oracles ne permettent pas de déposer des fonds et ne servent qu'à faire le lien entre la blockchain et le monde réel, cette métrique ne leur est pas applicable. Pour mesurer l'impact des oracles, nous utilisons la TVS qui signifie "**Total Value Secured**".

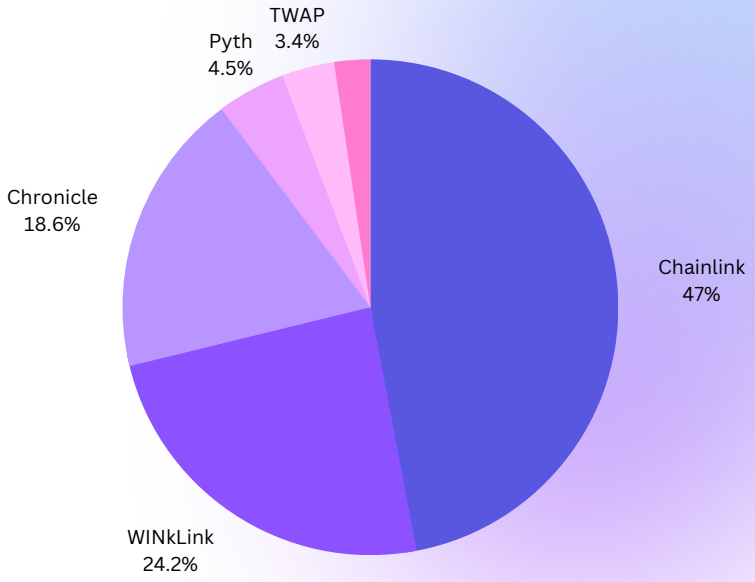
La TVS mesure la valeur totale des actifs déposés dans des smart contracts qui nécessitent les données des oracles pour s'exécuter.

Imaginons un coffre-fort où vous et votre ami stockez des cartes Pokémon rares. La TVL serait la valeur totale de toutes les cartes Pokémon que vous avez mises dans ce coffre-fort.

Un collectionneur dont le travail est d'estimer les cartes Pokemon vous communique les données sur le prix de la première carte qui vaut 50€ et sur la deuxième carte, 100€. Ce collectionneur ici représente l'oracle qui sécurise 150€ de valeur. La TVS de cet oracle est donc de 150€.

Dans le cas des oracles blockchain, la TVS représente donc la valeur totale des actifs ou des données qu'ils sécurisent à travers les smart contracts sur la blockchain.

Nom	TVS
Chainlink	$11,58b
WINkLink	$5,96b
Chronicle	$4,58b
Pyth	$1,10b
TWAP	$847m
Internal	$258m
RedStone	$83,3m
cLabs	$80,4m
UMA	$80m
Binance Oracle	$74,1m



Source : DefiLlama

Les oracles qui utilisent des providers de Data

"Aggréger et normaliser les données provenant de plus de 100 exchanges et des milliers de marchés actifs n'est pas simple. Cela nécessite un travail d'ingénierie approfondi et une surveillance constante pour garantir des données continues et de haute qualité, adaptées à une utilisation en entreprise.." - **Clara Medalie, Head of Research @ Kaiko**

Commençons par les oracles qui obtiennent leurs données grâce à des Data Providers, qui sont les plus courants dans notre écosystème. Nous l'avons vu précédemment, un oracle permet aux smart contracts d'accéder à des informations qui ne sont pas stockées sur la blockchain, élargissant ainsi les types et la quantité de données sur lesquelles un smart contract peut opérer.

Cette augmentation de la connectivité introduit de nouvelles vulnérabilités, nécessitant des mesures de sécurité renforcées pour garantir l'intégrité des fonctionnalités essentielles d'un smart contract, à savoir son exécution basée sur des données fiables.

Le transfert de données spécifiques et de haute qualité, sur lesquelles nous pouvons compter pour sécuriser des milliards de dollars, n'est pas une responsabilité à confier à la légère. L'enjeu majeur est d'acquérir rapidement des données précises en grande quantité et ce de manière sécurisée.

Pour atteindre cet objectif, il est dans l'intérêt des oracles que les nœuds s'approvisionnent directement auprès de fournisseurs de données renommés. Ces derniers, dotés d'équipes solides et d'une infrastructure robuste, se consacrent entièrement à la production de données de qualité pour leurs secteurs respectifs.

Il est important de comprendre que les oracles, dont la mission est de transmettre des données à la blockchain, s'approvisionnent auprès de sociétés nommées "Data Providers". Ces entités, qu'elles soient des organisations ou des entreprises, disposent d'une infrastructure adaptée pour communiquer des données ou des métadonnées aux oracles.

Certains fournisseurs offrent des données gratuitement, tandis que d'autres les monétisent. Bien que certains se spécialisent dans la collecte et la vente de données, de nombreuses disponibles proviennent d'entités diverses souhaitant partager ou capitaliser sur les informations générées par leurs activités quotidiennes.

Toute entité générant des données et prête à les distribuer peut se positionner comme fournisseur de données, à condition de répondre aux standards requis par les différents oracles qui souhaitent les utiliser.

Comment sont-ils sélectionnés ?

Nous l'avons évoquée précédemment, la génération de données n'est pas une tâche que l'on peut confier à n'importe qui.

403.2M

Fonds perdus avec la manipulation d'oracles en 2022

(environ 10% des fonds totaux hackés selon Chainalysis)

La manipulation des prix de l'oracle sous-entend que des personnes mal intentionnées ont manipulé le prix d'un actif. L'oracle a ensuite transmis ce prix manipulé au smart contract, permettant au hacker de s'approprier les fonds du protocole.

Note importante : la majorité des hacks associés à la manipulation des prix des oracles proviennent d'une mauvaise implémentation des données de l'oracle au sein des protocoles affectés.

Néanmoins, les oracles ont la responsabilité de vérifier que les flux de données transmis par les data providers **sont fiables et reflètent fidèlement les données réelles**, afin de prévenir toute manipulation et conflit d'intérêt.

Pour répondre à la question posée précédemment, les data providers sont choisis en fonction de leur réputation. Ils sont spécialisés dans la production de données de haute qualité et disposent de grandes équipes ainsi que d'une infrastructure full-stack.

Comment les data-providers obtiennent-ils leurs données ?

Les data providers collectent leurs données directement à partir de leurs services et de leurs clients, tels que les plateformes d'échange (Binance, Bybit, Bitstamp), les firmes de trading (Auros, Bitmart, Jane Street) et les market makers (Aquanow, DWF Labs, IMC).

Les oracles n'ont alors qu'à se connecter aux API, qu'elles soient publiques ou privées, mises à disposition par ces acteurs.

D'autres oracles peuvent aller chercher la data directement on-chain pour en faire l'agrégation et la fournir aux protocoles. Les oracles et data providers ne représentent donc qu'une seule entité et sont totalement autonomes.

Exemple d'oracle 1 : ChainLink - TVS : $11,446B

Chainlink occupe aujourd'hui une position dominante sur le marché des oracles décentralisés. Avec plus de 1800 intégrations et sa présence sur plus de 15 blockchains, ce réseau assure une connexion efficace et fiable entre les smart contracts et les sources de données externes. Le jeton $LINK sert d'incitation pour une prestation de services de qualité, garantissant ainsi la fiabilité des données pour les contrats intelligents.

Né en 2017 de l'initiative de Sergey Nazarov et Steve Ellis, Chainlink a progressivement consolidé sa position dominante en intégrant de nouvelles technologies et en publiant un second livre blanc en avril 2021. Ce dernier expose sa vision pour l'expansion des capacités des réseaux d'oracles décentralisés.

À ce jour, Chainlink collabore avec 98 Data Providers, allant des bases de données publiques aux sociétés de trading institutionnelles.

Exemple d'oracle 2 : Pyth - TVS : $1,092B

Présenté en début de ce dossier, Pyth Network est un oracle conçu pour fournir des données financières précises, sécurisées et instantanées aux blockchains et smart contracts. L'objectif principal de cet oracle est de résoudre le problème récurrent de la latence des données dans la DeFi en minimisant le chemin de transmission des données, afin de les délivrer instantanément aux utilisateurs finaux.

Pyth Network opère sur plus de 30 blockchains, y compris Ethereum, Binance Smart Chain et diverses blockchains de layer 2, grâce aux solutions créées par Wormhole.

Afin d'assurer la précision des données et la résilience face aux fournisseurs de données malveillants, Pyth Network utilise une méthode de "Price Aggregation". Cette méthode collecte, compare et arbitre les données fournies par divers fournisseurs, garantissant ainsi une donnée unique et fiable pour les consommateurs. Pyth Network constitue donc un lien direct et essentiel pour les Dapps au sein de l'écosystème DeFi.

Actuellement, Pyth Network collabore avec près de 100 Data Providers différents, allant des protocoles décentralisés aux entreprises spécialisées dans la collecte et l'analyse de données, telles que Kaiko.

VRF

Dans cet écosystème, principalement alimenté par le monde de la finance et des données numériques, les oracles ont également le rôle crucial d'introduire de manière fiable un élément capital dans la blockchain : le hasard.

Plus précisément, il existe des oracles appelés Oracles VRF (Verified Random Function), capables de générer des nombres aléatoires dont la nature imprévisible des résultats peut être prouvée cryptographiquement.

En effet, générer un véritable hasard sur la blockchain est un défi majeur pour les développeurs. Pour être considéré comme fiable, un nombre aléatoire doit être impartial, imprévisible, vérifiable et instantanément disponible. Néanmoins, en raison de la nature déterministe de la blockchain, obtenir un hasard suffisamment imprévisible s'avère souvent compliqué.

Pourquoi le hasard est-il important ?

Les applications blockchain ont fréquemment besoin de nombres aléatoires pour diverses fonctions, telles que la création de jeux, casinos, la répartition des tâches ou encore la génération aléatoire et la rareté dans les NFTs.

Voici comment fonctionnent les VRF :
1. Plusieurs paramètres d'entrée sont envoyés à un oracle VRF.
2. L'oracle VRF réalise des calculs sur ces entrées afin de générer des résultats pseudo-aléatoires.
3. Ces résultats sont vérifiables par quiconque et à tout moment grâce à la cryptographie.
4. Toutes les preuves sont publiées et vérifiées sur la blockchain avant que les applications ne soient autorisées à utiliser les résultats.

Prenons l'exemple d'un développeur de jeu de roulette sur la blockchain : pour garantir l'équité du jeu, il doit prouver que son algorithme est impartial et que la bille s'arrête de manière aléatoire sur une case. Plutôt que de dissimuler le processus, le développeur peut utiliser un oracle fiable pour démontrer comment les nombres aléatoires sont générés, assurant ainsi aux joueurs que le jeu est équitable.

De nombreux oracles offrent un service VRF, tels que Chainlink VRF, Binance Oracle VRF ou encore WinkLink VRF.

Exemple oracle VRF : WinkLink VRF - TVS : $5,997B

WINk est, à l'origine, une plateforme de jeu décentralisée. Elle a été la première DApp à être lancée sur la blockchain Tron en 2018 et la première plateforme de jeux à apparaître sur le Launchpad de Binance.

Le 26 avril 2021, WINk a acquis JustLink.io. Ce dernier est le premier projet officiel d'oracle décentralisé sur le réseau TRON, de cette fusion est né WinkLink. Il intègre toutes les fonctionnalités « primaires » d'un oracle, à savoir la diffusion de données du monde extérieur.

La particularité de WINkLink est sa capacité à fournir des nombres aléatoires fiables, imprévisibles et vérifiables. Cette fonctionnalité crée une belle synergie avec sa plateforme de jeu décentralisée !

Identity

Parmi les oracles spécifiques, nous pouvons également citer les dID qui relient les données d'identité du monde réel à la blockchain.

Ces derniers permettent la vérification de l'identité d'un utilisateur de manière privée, sans révéler d'informations personnelles. Grâce à des technologies avancées, certaines solutions KYC sont à la fois décentralisées et respectueuses de la vie privée, tout en étant conformes aux réglementations. Elles permettent ainsi aux protocoles de respecter les normes du web3 tout en se montrant prudents vis-à-vis des promesses de protection des données de certains fournisseurs.

Un exemple pratique: Jean souhaite utiliser une plateforme d'échange de cryptomonnaies conforme aux normes du web3.

Pour s'inscrire, la plateforme demande une vérification d'identité. Au lieu de fournir une copie de sa pièce d'identité ou d'autres documents sensibles, Jean fait appel à un oracle dID. L'oracle vérifie l'identité de Jean dans le monde réel et confirme à la plateforme que Jean est bien qui il prétend être, le tout sans jamais divulguer ses détails personnels à la plateforme. Ainsi, Jean peut utiliser la plateforme en toute sécurité, sachant que ses informations personnelles demeurent privées et protégées, tout en respectant les réglementations en vigueur.

Exemple oracle dID : zk.me

L'oracle zkMe est une solution avancée qui permet de partager en toute sécurité et confidentialité des informations d'identité vérifiées dans l'univers Web3. Il utilise des technologies sophistiquées telles que les preuves à divulgation nulle de connaissance (Zero-Knowledge Proof) et le calcul multipartite pour protéger la vie privée et la sécurité des utilisateurs. Contrairement aux systèmes traditionnels d'identification, zkMe donne aux utilisateurs le pouvoir de choisir quelles informations d'identité ils souhaitent partager avec des parties autorisées, leur offrant ainsi un meilleur contrôle sur leurs données personnelles. Ce processus de vérification flexible est adapté aux besoins des entreprises et fournit des informations utiles sur les utilisateurs sans compromettre leur confidentialité.

zkMe a gagné la confiance d'émetteurs, de détenteurs et de vérificateurs du monde entier, ce qui en fait un acteur clé dans la création d'un monde numérique sécurisé et respectueux de la vie privée.

Note importante : le risque de vol de données persiste avec ce genre de solutions. En effet, ce risque est simplement déplacé de la plateforme vers l'entité chargée de vérifier votre identité pour l'oracle.

Oracle de crédit

Nous nous concentrons ici sur les oracles spécifiquement dédiés au crédit et non sur les oracles classiques fournissant des prix qui sont ensuite utilisés par les protocoles de prêt et emprunt.

Un oracle de crédit dans la blockchain fait référence à un système qui fournit des informations sur la solvabilité ou la cote de crédit d'une entité (qu'il s'agisse d'une personne, d'une entreprise ou d'une autre entité) à des protocoles ou applications décentralisés.

Dans le contexte traditionnel, une cote de crédit est utilisée par les banques et autres institutions financières pour évaluer le risque associé au prêt d'argent à un emprunteur. Dans le monde de la blockchain, en particulier dans le secteur de la finance décentralisée (DeFi), la capacité de connaître la solvabilité d'une entité est tout aussi cruciale.

L'intérêt d'un oracle de crédit est multiple:

- Accès à des prêts sans garantie : Dans la DeFi, la plupart des prêts sont surcollatéralisés, ce qui signifie que les emprunteurs doivent déposer une valeur plus élevée que le montant emprunté pour garantir le prêt. Avec une évaluation fiable de la solvabilité, il est possible d'envisager des prêts avec un taux de collatéralisation moins élevé.
- Tarification basée sur le risque : En connaissant la cote de crédit d'un emprunteur, les prêteurs peuvent ajuster les taux d'intérêt en fonction du risque associé à chaque emprunteur.
- Expansion de la DeFi : En intégrant les concepts de notation de crédit, la DeFi pourrait attirer une plus grande partie de la population qui n'a actuellement pas accès aux services financiers traditionnels.

Intégration avec le monde financier traditionnel : Les oracles de crédit peuvent aider à établir un lien entre les systèmes financiers traditionnels et décentralisés, favorisant ainsi une adoption plus large de la blockchain.

Si les oracles de crédit vous intéressent, voici des projets qui pourraient vous intéresser : Credora, Spectral, CreDA ou encore LedgerScore.

Une place importante dans le monde des NFTs

Les oracles jouent un rôle essentiel dans le monde des NFTs, en particulier dans le secteur des jeux basés sur ces derniers.

Les oracles offrent aux développeurs de jeux NFT un pont pour accéder aux données du monde réel.

Concernant l'évaluation des prix : le marché des NFT est caractérisé par une liquidité souvent limitée, en partie car de nombreux NFT ont des caractéristiques uniques rendant leur évaluation particulièrement complexe. À l'heure actuelle, l'évaluation des NFTs fonctionne globalement à travers les Floor Prices et les offres disponibles.

Les oracles NFT ont un rôle crucial à jouer. Ces systèmes sont capables de retracer les anciennes transactions, permettant ainsi d'avoir un historique clair des valeurs précédentes d'un NFT. Ils sont également équipés pour "scraper", c'est-à-dire extraire des informations depuis les réseaux sociaux, les articles et d'autres sources en ligne pour déterminer la popularité et la perception d'un NFT donné.

Ces données, lorsqu'elles sont agrégées et analysées, offrent une évaluation beaucoup plus précise et fiable du prix en tenant compte aussi bien du passé que des tendances actuelles.

D'autre part, les oracles jouent un rôle fondamental dans la création de NFT dynamiques, marquant ainsi une évolution significative par rapport aux NFT traditionnels et statiques.
Ces NFT dynamiques sont des smart contracts qui utilisent des oracles pour interagir avec des données externes et s'adapter en fonction de celles-ci.

Prenons l'exemple d'une paire de chaussures de course en NFT. Imaginez que chaque fois qu'un athlète établit un nouveau record du monde sur 100 mètres, le design de ce NFT change pour refléter la vitesse ou les couleurs nationales du coureur. Si actuellement un athlète américain détient le record, le NFT afficherait un design bleu, blanc et rouge avec une étoile brillante. Si demain, un coureur jamaïcain bat ce record, le NFT se transformerait pour arborer les couleurs vert, jaune et noir avec un éclair.

D'autres exemples pratiques :

Vérification de l'Authenticité : Un collectionneur souhaite acheter un NFT représentant une œuvre d'art numérique. Avant de finaliser l'achat, la plateforme utilise un oracle NFT pour confirmer l'authenticité de l'œuvre et s'assurer qu'elle provient bien de l'artiste revendiqué.

Évaluation des Prix : Un joueur de jeu vidéo souhaite vendre un objet in-game sous forme de NFT. Pour déterminer le bon prix, la plateforme de jeu consulte un oracle pour lui donner le prix le plus fiable possible qu'elle peut aller chercher sur des marchés secondaires.

Traçabilité des Objets Physiques : Une entreprise revend des baskets de collection en édition limitée, chaque paire étant associée à un NFT. Grâce à un oracle, l'entreprise peut vérifier l'authenticité et la traçabilité de chaque paire de baskets.

Mise à Jour Automatique : Un jeu basé sur la blockchain offre des récompenses en NFT qui varient en fonction des événements mondiaux réels (par exemple, des tournois sportifs). Un oracle est utilisé pour mettre à jour automatiquement les récompenses en fonction des résultats de ces événements.

Conversion Monétaire : Un utilisateur souhaite acheter un NFT sur une plateforme mais le prix est indiqué dans une cryptomonnaie qu'il ne possède pas. Un oracle permet de fournir le taux de conversion actuel lui permettant de connaître le coût exact dans sa propre cryptomonnaie.

Droits d'Auteur : Un musicien met en vente ses morceaux sous forme de NFT. À chaque fois qu'un morceau est utilisé dans une publicité ou un film, un oracle détecte cette utilisation en 'scrapant' toutes les bandes originales des films et assure que les royalties sont correctement versées au musicien.

Ces cas d'usage montrent la polyvalence des oracles NFT et la façon dont ils peuvent être utilisés pour renforcer la confiance, la transparence et l'efficacité dans diverses applications de la blockchain.

Exemple d'oracle NFTs : DIA

DIA a développé un oracle qui fournit avec précision les floor prices des NFTs. Cette fonctionnalité ouvre de nombreuses possibilités dans cet univers comme les produits dérivés, le lending et le borrowing, le prêt de NFTs et le fractionnement.

Vous pouvez trouver plus d'exemples d'oracles NFTs proposés par DIA sur ce lien.

La sibylle de Cumes par Domenichino (1581-1641)

Chainlink : le monopole incontesté jusque-là

Pour bon nombre d'investisseurs en cryptomonnaie, certains incarnent leur catégorie d'actif. Ainsi, quand ils pensent à un stablecoin, c'est l'USDT de Tether qui leur vient à l'esprit. Binance est souvent la première plateforme d'échange à laquelle ils pensent. En matière d'oracle, Chainlink est la référence qui domine leurs discussions.

Ces entités sont perçues comme des leaders incontestés dans leurs domaines respectifs et il est courant que nous leur accordions une confiance presque instinctive. Cette confiance se manifeste tant dans nos décisions d'investissement que dans nos préférences pour des choix de partenariat.

Le succès de Chainlink a été garanti par son intégration dans de nombreux protocoles “blue-chip” de la finance décentralisée avec une TVL importante. De plus, sa robustesse a non seulement démontré sa résilience mais a également renforcé la confiance des investisseurs envers la précision de ses données et la fiabilité de sa solution.

Nous pouvons également parler **d’un First Mover Advantage**. Bien que Chainlink n’ait pas été le premier oracle, ce dernier a été le premier à proposer ses services à de multiples protocoles augmentant ainsi sa place dans la DeFi, le tout porté par une communauté très active sur les réseaux sociaux que l'on appelle couramment les "Link Marines

Ce monopole va-t-il se maintenir ?

“Je pense que Chainlink est cool et je suis content qu'il existe, bien que son modèle de sécurité soit trop centralisé pour que je sois satisfait qu'il soit la solution à tous les problèmes d'oracle. C'est génial comme une solution parmi plusieurs, de la même manière qu'il est bon d'avoir par exemple des stablecoins adossés à la monnaie fiduciaire comme une solution parmi d'autres. Je pense cependant que l'armée Twitter de Chainlink est vraiment amusante.” - **Vitalik Buterin sur Reddit à propos de Chainlink (2020)**

Voici quelques statistiques de Chainlink (au moment de la publication du dossier) :

46%
Part de marché

1800
Intégrations

+15
Blockchains

$7.8
Capitalisation du LINK (Milliards)

Compétition sur un nouveau terrain

Même si Chainlink domine actuellement le domaine des oracles, l'équipe ne compte pas s'arrêter en si bon chemin. Avec l'ascension fulgurante de multiples blockchains de niveaux L1 et L2, l'interopérabilité est devenue une pierre angulaire pour la plupart des intervenants de ce milieu.

De nombreuses solutions tentent de relever ce défi : que ce soit IBC (Inter Blockchain Communication) de Cosmos, les Parachains de Polkadot, Axelar, Thorchain ou encore LayerZero.

Récemment, Chainlink a dévoilé son initiative en matière d'interopérabilité avec le lancement du Chainlink CCIP (Cross Chain Interoperability Protocol). Cette solution a pour objectif de simplifier les échanges entre différentes blockchains. Ainsi, Chainlink ne se positionne plus uniquement comme un leader des oracles, mais aussi comme **un acteur incontournable de l'interopérabilité.**

Grâce à CCIP, des fonctionnalités telles que le prêt inter-blockchain, le transfert de fonds entre différentes blockchains, l'optimisation des rendements en exploitant les taux d'intérêt disparates entre blockchains et bien d'autres applications pourraient voir le jour.
Cependant, s'aventurer sur ce nouveau terrain signifie aussi affronter une nouvelle concurrence. Il est donc captivant d'observer comment Chainlink va naviguer dans ces eaux et si son emprise sur ce segment sera aussi marquante que celle qu'il a sur le monde des oracles.

Les nouveaux entrants

La sphère des oracles a connu une croissance fulgurante, passant de la modeste présence de **2 acteurs en 2020 à un impressionnant total de 46 oracles en date** de ce rapport, selon DeFi Llama. Cette évolution est principalement due à l'apparition de nouveaux besoins spécifiques aux diverses blockchains et protocoles, là où des oracles bien établis tels que Chainlink ou Chronicle ne sont pas encore présents.

Outre l'extension vers d'autres blockchains, les protocoles ont également des exigences plus nuancées. Par exemple, ils peuvent chercher une certaine forme de décentralisation, un modèle économique unique (comme le mécanisme de détention de tokens ou le mode de rémunération pour le service fourni) ou tout autre critère jugé crucial lors du choix d'un oracle.

La dynamique du marché s'est encore intensifiée avec l'entrée de géants technologiques comme Google. Des entreprises innovantes comme LayerZero semblent déjà prêtes à s'associer à des acteurs centralisés au détriment des solutions décentralisées, **en capitalisant sur la réputation solide** de ces derniers pour garantir la fiabilité des données dans l'univers du web3.

Le business model et son amélioration

Un modèle économique n'impliquant pas (ou très peu) l'utilisation d'un token est une quête qu'aucun projet n'a réussi à concrétiser.

D'après notre étude, le défi majeur pour Chainlink demeure **sa dépendance à la vente de ses tokens** pour financer ses opérations. Cette dépendance est un enjeu courant dans notre écosystème pour de nombreux acteurs. Actuellement, la principale source de revenus pour les équipes de Chainlink provient de la vente de ces tokens. La raison est simple : les revenus générés par les services de Chainlink ne suffisent pas à soutenir un modèle économique dépourvu de token.

Comme mentionné, Chainlink n'est plus seulement en concurrence avec d'autres oracles mais également d'autres solutions axées sur l'interopérabilité entre les blockchains, comme LayerZero par exemple.

Lorsqu'une entreprise s'aventure sur un marché plus large, elle se retrouve généralement face à une concurrence accrue et doit ainsi investir beaucoup d'argent pour se remettre à niveau.
Chainlink continue de puiser dans ses réserves de tokens pour compenser ses dépenses opérationnelles et assurer la rémunération de ses équipes.

Au mois de juin 2023, un modèle économique revisité a été proposé sur le blog de Chainlink. Baptisé "Sustainable Oracle Economics", ce dernier propose un certain nombre de changements qui concernent l'utilisation des tokens LINK par les équipes de l'oracle.

Dans cette publication, 3 mécanismes sont mis en avant pour augmenter les revenus de l'entreprise et diminuer les frais.

Augmentation de revenu :

- Paiement en fonction de l'utilisation : Chaque fois qu'un utilisateur paie les frais du protocole, une partie de ces frais serait également destinée à couvrir le coût de l'utilisation de l'oracle par ledit protocole.
- Partage de frais : Chainlink pourrait recevoir une portion des revenus générés par les frais des protocoles qui utilisent l'oracle. Par exemple, GMX a convenu de reverser 1,2% des frais collectés de sa V2 à Chainlink.
- Chainlink BUILD : Destiné aux protocoles en phase initiale, ce programme leur permettrait d'accéder aux services de Chainlink en échange de l'allocation de 3 à 7% de leur supply totale de tokens à Chainlink.

Réduction des frais :

- OCR 2.0 : Agrégation des données collectées et soumission de ces dernières en une seule transaction après consensus.
- Oracles de basse latence : Utilisation de la data off-chain uniquement lorsque le besoin se présente. Cela inclut le paiement de gas qui serait déplacé de Chainlink vers les utilisateurs ou les protocoles.
- La dépréciation du feed : Élimination des feeds de data qui sont peu utilisés, ne sont pas viables sur le long terme ou n'ont pas d'utilisateurs. Ces derniers pourraient être relancés si le besoin se représentait.

Vous retrouverez notre analyse détaillée sur l'évolution du positionnement de Chainlink par rapport aux autres oracles dans la partie Perspectives du document.

LES TOKENS D'ORACLES

Bien que les fonds levés soient considérables et l'intérêt des investisseurs indéniable, la majorité des participants de l'écosystème crypto demeure profondément sceptique envers l'utilisation des tokens comme moyens de financement.

Le paysage est parsemé de fraudes, d'opérations douteuses et d'entreprises faisant preuve de dépenses exorbitantes, créant un environnement parfois plus que chaotique pour les investisseurs.

Une question cruciale persiste : **les financements par tokens présentent-ils une réelle valeur pour le projet et les souscripteurs ?**

Au-delà de leur rôle en tant que moyens de financement, il est essentiel **de souligner l'utilité des tokens au sein des oracles blockchain.** Ces tokens servent non seulement d'incentive pour encourager l'accès à des données précises et fiables mais ils agissent également comme mécanisme de mise en jeu (staking) pour garantir l'intégrité des informations fournies.

De plus, ils peuvent être utilisés comme moyen de paiement pour accéder aux services d'oracle et participer à la gouvernance du réseau permettant alors aux détenteurs de tokens d'avoir un mot à dire dans l'évolution du système.

Enfin, dans un univers où la confiance est décentralisée, les tokens contribuent à établir et à mesurer la réputation des fournisseurs d'oracle. À ce titre, ils s'avèrent être un composant primordial à cet écosystème ajoutant une couche de sécurité et de fonctionnalité qui va au-delà de la simple levée de fonds.

Tout cela semble bien utile, cependant, comment se fait-il que certains projets d'oracles arrivent à se passer d'un token ?

Dans cette partie, nous aborderons les modèles de tokenomics présents dans l'univers des oracles, les intérêts proposés et les risques associés. Enfin, nous engagerons une réflexion sur la pertinence de l'introduction d'un token dans un projet d'oracle.

À QUOI SERVENT LES TOKENS D'ORACLES ?

Nous l'avons vu dans l'introduction, les tokens occupent une place centrale dans l'écosystème des oracles blockchain. Ils semblent incarner la colonne vertébrale des interactions assurant l'intégrité, la sécurité et la fluidité des échanges d'informations entre le monde réel et la blockchain.

L'utilité d'un token se divise en 5 grandes catégories.

Financement du projet

L'argent étant le nerf de la guerre, le leader du marché Chainlink utilise son token afin de financer ses énormes besoins en recherche et développement.

A titre d'exemple, le portefeuille Chainlink "Noncirculating Supply" a déposé 15,7 millions de $LINK (97,5 millions de dollars) sur Binance le 16 septembre 2023 et ce, tous les trois mois depuis le 26 août 2022 pour un montant total de 71.8M $LINK ($446M) !

Comme mentionné dans un récent article de blog concernant l'approche de Chainlink en matière d'économie d'oracle, la Fondation vise à établir un calendrier de libération de tokens plus prévisible et à plus long terme afin de créer plus de clarté pour la communauté.

Il est intéressant de noter que la genèse des oracles coïncide de près avec la naissance de la DeFi.

"Sans oracles AAVE n'existerait pas aujourd'hui. Sans oracles la DeFi ne serait pas telle qu'on la connaît aujourd'hui" - **Marc Zeller, Founder AAVE Chan Initiative**

À cet instant, les oracles ne pouvaient pas espérer exister sans un accès direct au financement via les ventes d'un token car les protocoles DeFi n'étaient pas en capacité de les rémunérer.

Ce paysage a depuis évolué et les revenus des protocoles ont augmenté. On peut donc espérer voir les oracles réduire leur dépendance sur les ventes de jetons tout en étant capables de se rémunérer grâce au service qu'ils apportent à l'avenir.

Moyen de paiement

Les tokens d'oracles peuvent également être utilisés en tant que moyens de paiement.

Ces derniers peuvent par exemple servir à payer les opérateurs de nœuds pour accéder au service de l'oracle. Cela permet d'augmenter la demande pour le token, augmentant ainsi son prix et rendant le système plus résilient.

D'un autre côté, cela permet aux opérateurs de nœuds d'augmenter leur quantité de jetons qu'ils stakent, accentuant ainsi leur capacité à subir des sanctions (slashing) et avoir plus de délégations sur leurs nœuds. Nous allons expliquer ce fonctionnement ci-dessous.

Incentive à fournir des données de qualités

En tant qu'incentive, les tokens encouragent la transmission de données précises et fiables.

Dans le monde sans confiance (trustless), les participants et acteurs actifs doivent avoir des mécanismes les empêchant de manipuler le réseau, être inactifs ou tout simplement profiter de leur position.

Nous pouvons ainsi voir rapidement l'utilité des tokens pour les bons et les mauvais acteurs : nous allons aborder le staking et le slashing, les deux principaux mécanismes d'incentives pour toutes les personnes et protocoles utilisant les oracles.

Staking

Le staking permet aux investisseurs de générer un intérêt sur la détention du token en recevant des récompenses supplémentaires sous forme de nouveaux tokens, augmentant ainsi leur solde total.

Les utilisateurs peuvent décider de déléguer leurs tokens aux fournisseurs de données (nœuds) en lesquels ils ont le plus confiance, diminuant potentiellement leur risque de perte de fonds. Ce processus peut cependant poser des risques de centralisation c'est pourquoi différents mécanismes permettant la régulation de cette centralisation peuvent être mis en place.

Les bons acteurs sont gagnants car en ayant plus de délégation, ces derniers profitent des commissions tout en générant des revenus de leur service de base.

Le staking permet de générer des intérêts de deux façons :

- L'inflation inhérente à la blockchain prévue dans les tokenomics
- Les intérêts supplémentaires reversés avec les revenus générés par l'activité de l'oracle

La façon dont les intérêts sont générés est définie par l'équipe derrière l'oracle ou par le vote d'une DAO.

Slashing

Le slashing va pénaliser les acteurs qui n'effectuent pas correctement leur travail.

Examinons comment cela fonctionne et pourquoi, en tant que particulier, vous pourriez perdre de l'argent à cause du slashing dans le contexte des oracles.

Pour assurer l'intégrité des données, de nombreux oracles utilisent un système dans lequel les fournisseurs de données (ou nœuds d'oracle) doivent mettre en jeu des tokens en tant que garantie. Si un fournisseur de données ou un nœud fournit des informations incorrectes ou malveillantes, il risque de se faire "slasher", c'est-à-dire de perdre une partie ou la totalité des tokens mis en jeu.

Plusieurs motifs peuvent entraîner le slashing d'un nœud d'oracle :

- Données incorrectes : Si un oracle fournit des données qui sont prouvées comme étant inexactes ou trop éloignées des autres fournisseurs de données, il peut être pénalisé.
- Comportement malveillant : Toute tentative de manipulation des données, d'influence indue sur un smart contract, ou d'autres actes malveillants peuvent entraîner un slashing.
- Downtime prolongé : Si un oracle ne parvient pas à fournir des données de manière régulière, cela peut être considéré comme un manquement à ses obligations et peut entraîner une pénalité.

À noter que le slashing n'est pas "fatal". Pour la plupart des oracles, ce slashing est progressif et augmente avec le nombre de données faussées et inexactes ou le temps d'activité. Chaque oracle définit son propre fonctionnement de slashing.

Participation à la gouvernance

Enfin, les tokens jouent un rôle déterminant dans la gouvernance des oracles, permettant aux détenteurs d'influencer le développement et l'évolution de chaque système.

Il est toutefois important de préciser que ces systèmes de gouvernance ne sont pas présents dans tous les protocoles et relèvent bien souvent de la volonté des fondateurs.

EXEMPLES D'UTILISATION

Chainlink

Concernant Chainlink, la supply est bloquée à un milliard de jetons. Les entreprises ont besoin de jetons $LINK pour payer les opérateurs de nœuds. Ces derniers auront également besoin de réserve de token $LINK afin de répondre aux demandes qui nécessitent une garantie.

Dans le futur, des opérateurs de nœuds ouverts existeront, facilitant les dépôts des utilisateurs. Ces derniers verseront des intérêts sur les montants déposés par les utilisateurs. Cette approche permettra la constitution d'une pool de tokens par les opérateurs de nœuds, soutenant ainsi plusieurs accords de garantie simultanément. À ce niveau, il y a une incitation pour les opérateurs de nœuds, les investisseurs et les entreprises à posséder des réserves de tokens $LINK.

En 2017, l'ICO a permis à Chainlink de lever 32 millions de dollars. Au total, 35% de l'offre totale de 1.000.000.000 LINK a été distribuée aux investisseurs, pour un prix moyen de vente de token LINK de 0,091$.

À l'heure où nous écrivons ces lignes, CoinMarketCap place $LINK 19e au classement crypto-monnaies. Le token a une capitalisation boursière de 4,1 milliards de dollars et une offre en circulation de 556 millions de jetons. Le prix du LINK est de 7,4 dollars par token.

Band Protocol

Au sujet de Band Protocol, l'oracle a été fondé en 2019 en Thaïlande par trois informaticiens. À l'origine, Chainlink était un oracle spécifique à Ethereum et ne pouvait donc servir que les applications basées sur cette blockchain. Band a donné le coup d'envoi de l'interopérabilité en mélangeant les applications basées sur Ethereum, Polkadot, Icon, Tron, Solana et Cosmos. Le protocole étant construit sur le SDK Cosmos, il tire parti de la faible latence et du haut débit de Cosmos pour maintenir les coûts à un niveau bas pour les applications gourmandes en données.

BAND a également lancé sa propre blockchain, devenant ainsi le token natif du réseau Band Protocol. Tout d'abord, comme pour le LINK, le staking est possible en tant que nœud validateur. Cependant, devenir un validateur BAND nécessite des compétences techniques et une grande quantité de tokens BAND puisque seuls les 100 plus gros validateurs BAND sont éligibles pour sécuriser la blockchain. Le validateur est responsable de l'ajout de nouveaux blocs sur la BandChain et la participation au consensus.

En plus d'être utilisé pour le staking, BAND est également un token de gouvernance. En tant que détenteur de BAND, vous avez le droit de proposer et de voter sur des référendums au sein du réseau. Des votes sont régulièrement organisés pour décider de l'utilisation des fonds de la réserve communautaire.

La réserve communautaire est financée à 2% des récompenses de bloc de la BandChain. Ainsi, l'objectif principal de la réserve communautaire est de soutenir des initiatives portées par celle-ci visant à étendre l'écosystème Band.

En 2019, Band Protocol a réalisé une ICO pour ses tokens BAND générant au passage 5,85 millions de dollars. L'ICO de Band Protocol a eu lieu sur Binance Launchpad. Au moment de l'ICO de ses tokens BAND, l'offre de BAND était de 100 millions de tokens. Une vente privée de 2 millions de dollars de tokens BAND a également été réalisée.
À l'heure où nous écrivons ces lignes, CoinGecko classe $BAND à la 188e place en termes de capitalisation. Le token a une capitalisation boursière de 140 millions de dollars et une offre en circulation de 134 millions de jetons. Le prix du BAND est de 1,04 dollars par token.

Tellor

Notre dernier exemple portera sur le protocole Tellor, l'oracle le "plus décentralisé" mais également celui qui a rencontré de nombreux soucis dernièrement. Le protocole est récemment passé d'un Proof-of-Work à un Proof-of-Stake et s'inspirait à l'origine des tokenomics simples mais très efficaces de Bitcoin.

L'objectif du token $TRB est d'aligner les intérêts des data providers, investisseurs et protocoles se servant des données de l'oracle. Les data providers de Tellor doivent staker des tokens $TRB en guise de gage de confiance.

En cas d'un mauvais reporting de données, n'importe quel utilisateur peut signaler le problème et mettre en jeu un 'dispute fee'. Si ce dernier a raison, il remporte ces tokens $TRB depuis le stake du fournisseur de données.

Tellor n'a pas réalisé d'ICO et il n'y a pas eu de pré-minage. Actuellement, CoinGecko positionne $TRB 234e au classement des crypto-monnaies. Le token a une capitalisation boursière de 97 millions de dollars et une offre en circulation de 2,5 millions de jetons. Le prix du TRB est de 38,8 dollars par token.

INTÉRESSANT POUR LES PARTICULIERS ?

En tant que particulier, détenir des tokens d'oracles relève de de la spéculation et d'un pari sur la prise de valeur de ces derniers. Cette partie ne constitue pas un conseil en investissement mais vise à donner une vue globale sur les opportunités et risques présents.

Cependant, si les roadmaps qui promettent une redistribution des revenus sont respectées, les particuliers détenant ces tokens seront les premiers à en profiter.

LES RISQUES DES TOKENS D'ORACLES

Dans l'écosystème vaste et diversifié des cryptomonnaies, les tokens d'oracle se démarquent avec des utilités bien spécifiques en fonction de chaque projet. Cependant, cette distinction ne les exempte pas de défis et de risques.

Les risques classiques des tokens

Les tokens d'oracle, comme tout autre token de façon générale, comportent des risques :

Volatilité : Le marché des cryptomonnaies est volatil. La valeur des tokens d'oracle peut fluctuer rapidement en fonction de la demande du marché, des perceptions des investisseurs ou à la suite d'événements liés à l'oracle lui-même. Par exemple, un oracle majeur annonçant une mauvaise intégration pourrait entraîner une chute rapide de la valeur du token.

Sécurité : Les tokens d'oracle, tout comme d'autres tokens, peuvent être la cible d'attaques malveillantes, telles que des hacks, des escroqueries ou des vols. Un oracle, de par sa fonction essentielle dans le bon fonctionnement des contrats intelligents, pourrait non seulement perdre des fonds s'il est compromis mais aussi impacter la confiance des utilisateurs et donc la valeur du token associé.

Liquidité : Tous les tokens ne jouissent pas de la même liquidité. Certains tokens d'oracle pourraient être peu échangés ou listés sur un nombre limité de plateformes. Cela pourrait rendre difficile la vente des tokens, en particulier lors de mouvements brusques du marché.

Réglementation : Les tokens, y compris ceux des oracles, peuvent être soumis à des réglementations strictes dans certaines juridictions. Si un gouvernement décidait de réguler ou d'interdire l'utilisation d'oracles ou de leur token, cela pourrait avoir un impact négatif sur leur valeur et leur utilisation.

Slashing

Le slashing peut impacter directement les utilisateurs de tokens et ce de plusieurs façons :

- Participation directe : Si vous mettez en jeu vos tokens d'oracle pour fournir des données, que vous commettez une erreur ou que vos données sont jugées inexactes, vous risquez de subir un slashing.
- Délégation à des fournisseurs d'oracle : Si vous déléguez vos tokens à un fournisseur de données et que ce dernier est pénalisé, vos tokens délégués pourraient également être touchés.
- Répercussions sur le marché : Un incident majeur affectant la confiance en un oracle particulier, tel qu'un événement de slashing important, peut diminuer la valeur du token associé même si vous n'avez pas été directement affecté.

Centralisation de la gouvernance :

Le niveau de centralisation de la gouvernance peut avoir des implications majeures pour la sécurité, la fiabilité et la transparence des oracles. Voyons comment la centralisation de la gouvernance impacte spécifiquement les tokens d'oracle.

La centralisation de la gouvernance fait référence à la concentration du pouvoir décisionnel entre les mains d'un petit groupe d'individus ou d'entités. Dans le contexte des oracles, cela pourrait signifier que quelques parties prenantes majeures (par exemple, des détenteurs de tokens influents, des fondateurs ou des investisseurs clés) prennent des décisions qui affectent l'ensemble du réseau d'oracle.

Les risques Associés à la Centralisation :

- **Intégrité des données :** Si un petit groupe contrôle la gouvernance, il peut influencer ou manipuler les données fournies par l'oracle pour leur bénéfice, compromettant ainsi le principe d'objectivité et de fiabilité.

- **Vulnérabilités de sécurité :** Une gouvernance centralisée peut devenir un point de défaillance unique. Si ce groupe est compromis, l'ensemble du réseau d'oracle peut être mis en danger.

- **Manque de transparence :** La prise de décision par un petit groupe peut manquer de transparence, ce qui peut entraîner une perte de confiance parmi les utilisateurs et les détenteurs de tokens.

- **Résistance à l'innovation :** Une gouvernance centralisée peut être réticente au changement ou à l'adoption de nouvelles technologies et méthodes, ce qui pourrait freiner la progression et l'adoption de l'oracle.

La centralisation de la gouvernance peut avoir un impact direct sur les détenteurs de tokens d'oracle :

- **Valeur du Token :** Si la communauté perçoit que l'oracle est dirigé par un petit groupe sans considération pour les besoins plus larges de la communauté, cela pourrait diminuer la confiance et donc la valeur du token.

- **Pouvoir Décisionnel :** Les détenteurs de tokens pourraient se sentir exclus du processus de prise de décision, rendant leurs investissements moins influents et potentiellement moins pertinents.

- **Incertitude :** La centralisation peut entraîner des décisions imprévisibles ou arbitraires qui peuvent surprendre les détenteurs de tokens et affecter leur stratégie d'investissement.

Un aspect particulièrement préoccupant de la centralisation de la gouvernance, surtout dans le monde des oracles, est la possibilité de conflits d'intérêt. Si un petit groupe contrôle la prise de décision, il est possible que leurs intérêts personnels ou commerciaux influencent leurs décisions, même si ces intérêts sont en conflit avec le bien-être global du réseau d'oracle.

Par exemple, un fournisseur d'oracle dominant pourrait avoir des liens financiers avec une entreprise externe. Si cette entreprise bénéficie d'une certaine manière des données transmises par l'oracle, le fournisseur pourrait être incité à manipuler ou à filtrer ces données pour favoriser cette entreprise. De tels actes nuiraient à la confiance des utilisateurs dans l'oracle et pourraient dévaloriser les tokens associés.

De plus, dans une gouvernance centralisée, les décisions concernant les partenariats, les intégrations ou les mises à jour technologiques pourraient être influencées par des affiliations personnelles ou commerciales plutôt que par ce qui est le plus favorable à l'oracle et sa communauté.

C'est pourquoi une transparence totale dans la prise de décision et une gouvernance décentralisée peuvent aider à atténuer ces risques potentiels de conflits d'intérêt, assurant ainsi que l'oracle fonctionne dans le meilleur intérêt de l'ensemble de sa communauté.

LES DEFIS ET LES CHALLENGES

Pour exploiter pleinement les avantages de la Finance Décentralisée, il est essentiel d'avoir des solutions d'oracle à la fois sûres et fiables. **Dans n'importe quel système financier, la confiance est primordiale et la DeFi ne fait pas exception.** Les utilisateurs doivent être assurés de la justesse et la fiabilité des informations transmises par les oracles.

Étant donné le caractère décentralisé de la DeFi, ce milieu est devenu une cible de choix pour les hackers et autres entités malintentionnées. **Compromettre un seul oracle peut entraîner des conséquences catastrophiques pour tout l'écosystème.** Il est donc impératif d'adopter des mesures de sécurité solides, comme le chiffrement et la validation par multi-signatures.

Dans cette partie nous allons revenir sur les défis liés aux oracles, les événements passés ainsi que les axes d'amélioration possibles.

VECTEURS DE VULNÉRABILITÉ

En 2023, le groupe de hackers nord-coréen Lazarus a orchestré des cyberattaques entraînant des pertes de 3,4 milliards de dollars dans notre écosystème. Saisir l'ampleur de cette problématique est crucial : selon Chainalysis, les attaques visant les oracles ont coûté **403,2 millions de dollars en pertes en 2022.**

Comment ces pirates parviennent-ils à exploiter les oracles pour réaliser de tels gains?

Dans les sections qui suivent, une exploration détaillée des techniques d'attaque ciblant différents types d'oracles et leur fonctionnement seront présentés.

Manipulation de prix

La distorsion du prix d'un actif découle généralement de deux facteurs principaux :

- L'utilisation d'une unique source de prix, vulnérable aux interférences d'acteurs malintentionnés.
- Une faille dans le code permettant son exécution continue même en présence d'anomalies dans le prix de l'actif.

L’infrastructure off-chain

Puisque les oracles fournissent les données du monde réel aux smart contracts, ces derniers doivent être connectés d’une manière ou d’une autre à des logiciels “traditionnels”.

Ainsi, tous les vecteurs de hacks liés à ces logiciels touchent le bon fonctionnement de l’oracle lui-même.

Cela inclut mais n’est pas exhaustif :

- Les accès au logiciel
- Social Engineering
- Leaks de données
- Faillite du hardware

Pour contrer ces problèmes “traditionnels”, il faut des mesures... traditionnelles.
Cela comprend des audits du code, des formations de cybersécurité des employés, des backups des serveurs et toute autre mesure faisant partie des bonnes pratiques à respecter dans l’univers du numérique.

La confiance en une entité centralisée

Les oracles puisent dans diverses sources d'information, appelées fournisseurs de données (Data Providers), pour transmettre les données à la blockchain.

La plus grande vulnérabilité des oracles est la confiance **qu’ils accordent à des Data Providers centralisés.**

Bien que la plupart des Data Providers soit des entreprises réputées et sélectionnées selon un certain nombre de standards, ces derniers sont sujets à des risques off-chain qui pourraient compromettre la fiabilité des oracles.

Les risques de la décentralisation

Dans le modèle centralisé, la principale vulnérabilité repose sur la confiance accordée à une seule entité. Pour le modèle décentralisé, le problème se concentre sur le système de rémunération.

En effet, le moteur principal des choix décentralisés provient de l’avidité des participants. Il est donc nécessaire d'examiner la manière dont ces acteurs sont récompensés mais aussi sanctionnés par l'oracle.

Si l'oracle rémunère les providers de data en fonction du volume des données fournies, **la quantité primera sur la qualité.**

De plus, les sanctions ou pénalités appliquées par l'oracle pour la diffusion de mauvaises données pourraient s'avérer trop légères, rendant les récompenses bien plus attractives que les risques encourus pour des comportements malveillants ou non conformes. Nous reviendrons sur ces sanctions un peu plus tard dans le dossier.

Freeloading

Le "Freeloading" est une forme de paresse ou d'opportunisme. Quand un nœud est payé pour fournir une donnée spécifique, il peut choisir de simplement se reposer sur une API publique ou d'utiliser une autre méthode qui coûte **moins cher que la rémunération qu'il reçoit, maximisant ainsi ses profits.**

Non seulement cette approche risque de centraliser la source de l'information mais elle est également susceptible d'introduire des retards dans la mise à jour des données.

Prenons un exemple :

- Le nœud A est payé par un protocole pour fournir le prix de l'ETH avec une exigence de mise à jour toutes les 10 minutes.
- Pour économiser des coûts, le nœud A décide de sous-traiter cette tâche au nœud B, qui offre un tarif moins élevé mais met à jour ses données seulement une fois par heure.
- Le nœud A rapporte le même prix pour l'ETH six fois en une heure.
- Si le marché de l'ETH connaît une chute soudaine ou une volatilité accrue durant cette période, des bots ou des traders en arbitrage pourraient exploiter cet écart de prix. Cela pourrait entraîner des pertes pour le protocole et ses utilisateurs qui s'appuient sur des données obsolètes.

Mirroring

Le "mirroring" est une tactique qui ressemble au "freeloading" mais avec une complexité supplémentaire. Lorsqu'un nœud choisit de se fier à une source d'information centralisée au lieu de collecter l'information lui-même, il ne s'arrête pas là. Il réplique ensuite cette donnée et la distribue à plusieurs autres nœuds. Ces derniers, à leur tour, soumettent la même information. Cette redondance dans la soumission amplifie les récompenses car chaque nœud est rémunéré pour la soumission de données, même si ces données proviennent d'une source unique.

Cela pose un sérieux problème car, au lieu d'avoir **une multitude de sources indépendantes** apportant de la diversité et de la robustesse à l'information sans communiquer entre elles, on se retrouve avec de multiples répliques de données provenant d'une seule source. Cela accroît la vulnérabilité car si cette source unique est compromise, tous les nœuds qui s'appuient sur elle pour le "mirroring" propageront des informations erronées ou malveillantes. Cela diminue alors la résilience du système d'oracle et expose les utilisateurs à des risques accrus.

LES BUGS ET HACKS

Dans cette partie, nous allons revenir sur les attaques qui ont eu lieu sur des oracles au sein des différents protocoles décentralisés. Nous commenterons également les reproches faits aux oracles réputés en apportant des explications poussées nécessaires à l'analyse des risques présents.

“It’s not a bug, it’s a feature” : Le multisig

Le multisig est une étape de sécurité supplémentaire très commune dans le monde décentralisé. Le principe est simple : afin d’effectuer une action quelconque, **le smart contract a besoin de plusieurs signataires**. Chaque smart contract définit ses propres besoins. Par exemple, Chainlink a besoin de 4 signatures sur 9 pour effectuer une action via son multisig.

Le multisig n’est pas utilisé à chaque envoi de données aux smart contracts. Il est utilisé pour mettre à jour ou intervenir sur le protocole en cas de besoins majeurs. Par exemple : rebranding d’un token, upgrade d’un smart contact, bug sur un protocole…

La décentralisation des oracles est un sujet qui suscite énormément de polémiques et de débats. Au cœur de ces derniers se trouve le multisig des différents projets ainsi que son utilisation par leurs fondateurs.

Chris Blec, figure proéminente de l’écosystème, s’est exprimé à de multiples reprises sur les dangers que représente le multisig de Chainlink pour l'ensemble de la Finance Décentralisée. Le fervent défenseur de la décentralisation décrit régulièrement sur les réseaux sociaux ce manque et cette menace qui pourrait peser sur les systèmes décentralisés.

Pour éliminer tout risque de centralisation lié au multisig, certains acteurs ont décidé de s’en débarrasser.

C'est le choix qu'a fait l'oracle Tellor, en détruisant ses admin keys et devenant ainsi complètement décentralisé. Les admin keys permettent à leurs détenteurs d’upgrade le contrat et d’en modifier certains paramètres.

Ne plus avoir d’admin keys confère plusieurs **avantages** aux projets :

- Éviter de se faire hacker ses admin keys et risquer la manipulation de contrats
- Remettre la gouvernance et la prise de décision au sein du protocole aux holders du token
- Entretenir les valeurs de la DeFi en supprimant un intermédiaire de confiance

Ne plus avoir d’admin keys crée cependant des **problèmes** :

- En cas de bug (voir l’exemple de Tellor), les contrats ne peuvent pas être mis à jour directement ce qui peut mettre les utilisateurs et leurs fonds à risque
- Bien qu’un mécanisme de sanction (type slashing) soit en place, la manipulation d’un oracle peut fortement affecter un protocole même si les mauvais acteurs sont punis

Le multisig reste donc une solution privilégiée par la plupart des oracles (sauf Tellor et Uniswap v3 TWAP) selon l’étude de Liquity. Chaque méthode a ses avantages et ses inconvénients et il est encore difficile de dire quel serait le choix optimal dans le contexte actuel.

L’implémentation d’un oracle au sein d’un protocole

Lorsqu’un feed de données est intégré au sein d’un protocole, les développeurs doivent prendre en compte de nombreux paramètres pour minimiser les vecteurs d’attaque possible.

La plupart des hacks de protocoles qui ont été effectués sur les données provenant d’oracles ne proviennent pas des oracles eux-mêmes, mais d’un morceau de code qui ignore certaines recommandations basiques.

On peut citer quelques exemples comme BonqDAO, Deus DAO ou encore Compound.

Il est important de souligner l'importance des audits internes et externes pour tous les protocoles. Nous avons échangé sur ce sujet avec Mudit Gupta, CSO de Polygon lors d'une interview à l'ETHCC 2023. Vous pouvez retrouver cette interview passionnante ici.

Les flash loans

L'attaque la plus fréquente sur les oracles est réalisée à l'aide des flash loans. Pour mieux comprendre ce type d'attaque, il est important de connaître ce mécanisme essentiel à la finance décentralisée.

Un flash loan permet à un utilisateur **d'emprunter instantanément et sans garantie une grande quantité d'actifs**, à condition que ces actifs soient remboursés dans la même transaction. Si les actifs ne sont pas remboursés à la fin de la transaction, celle-ci est annulée et la situation revient à l'état initial.

Prenons un exemple :

1. Vous remarquez une différence de prix entre l'ETH sur Sushiswap (1100$) et Uniswap (1000$)
2. Vous effectuez un flashloan de 1 Million d'$USDT
3. Vous utilisez ces $USDT pour acheter 1000 $ETH sur Uniswap
4. Vous les revendez sur Sushiswap contre 1.1 Million d'$USDT (moins les frais des deux DEX)
5. Vous remboursez 1M d'$USDT de Flash loan et empochez la différence

Ces flashloans peuvent être réalisés depuis des plateformes comme AAVE par exemple.

Les flash loans ont été initialement introduits dans le monde de la DeFi comme un moyen innovant d'effectuer des arbitrages entre différentes plateformes sans avoir à mettre en jeu son propre capital. Cette capacité à emprunter d'importantes sommes d'argent sans garantie préalable, à condition que l'emprunt soit remboursé dans la même transaction, a offert des opportunités d'arbitrage considérables.

Cependant, l'arrivée des Market Makers, du High Frequency Trading (HFT) et des bots a rendu l'utilisation des flashloans de plus en plus compliquée pour l'arbitrage.

Comment les oracles sont-ils manipulés à travers les flash loans ?

La multiplication du nombre de protocoles et blockchains a déclenché la multiplication du nombre de tokens et d'utilités. De nombreux tokens peuvent servir de collatéral pour des prêts décentralisés ou être intégrés dans des protocoles pour d'autres cas d'usage.

Lorsque l'oracle d'un protocole est mal configuré, un flash loan permet à un acteur de manipuler le prix d'un token à faible liquidité grâce à un échange massif de cryptomonnaies empruntées.

Nous vous recommandons de lire l'"article de blog de samczsun si vous souhaitez en savoir plus.

REGLEMENTATION DES ORACLES

La blockchain est souvent mise en avant pour sa transparence, sa décentralisation et sa résistance à la censure. Cependant, l'apparition des oracles en tant que canaux d'information, introduit un point potentiel de vulnérabilité. Par conséquent, la réglementation autour des oracles devient cruciale. D'une part, elle vise à garantir l'intégrité, la fiabilité et la sécurité des données transmises, d'autre part, elle cherche à prévenir d'éventuels abus ou manipulations qui pourraient compromettre l'intégrité des contrats intelligents et des applications décentralisées qui dépendent de ces données.

Avec l'évolution rapide des marchés financiers décentralisés (DeFi) et l'émergence d'autres secteurs basés sur la blockchain, la demande pour des données externes fiables et sécurisées accroît de jour en jour. **Une réglementation solide garantira non seulement la confiance dans les systèmes basés sur la blockchain mais facilitera également leur adoption à grande échelle**, en assurant aux utilisateurs et aux investisseurs que les informations qui alimentent ces systèmes sont exactes et fiables.

EN EUROPE

Le vieux continent est déjà au fait du rôle des oracles au sein de la finance décentralisée. Dans sa constante recherche de régulation autour de la DeFi, ses législateurs y voient certes une utilité mais surtout des risques issus du domaine cyber et de manipulations de prix.
Selon un rapport de Chainalysis sur l'année 2022 que nous avons cité plus haut : 403.2 millions de dollars dans l'écosystème DeFi ont été perdus du fait d'attaques via manipulations d'oracles.

L'Approche des régulateurs français par le risque

Un risque double, selon les régulateurs français :

Un risque pointé par l'ACPR, le risque cyber

Pour rappel l'autorité de contrôle prudentiel et de résolution (ACPR), dépendant directement de la Banque de France, est le régulateur français des établissements de crédit et des assurances. Il est également garant de la surveillance du respect des règles anti-blanchiment imposées aux prestataires de services cryptos en France.

Le risque cyber touchant à la vulnérabilité d'un système d'informations permet d'exploiter la vulnérabilité d'un actif.

C'est durant un discours à la « World Bank Global Payments Week » en mai 2023 que Monsieur Denis Beau, Premier sous-gouverneur de la Banque de France déclare :

« Le risque cyber constitue aujourd'hui le premier risque opérationnel pour les acteurs financiers, et il a la capacité de compromettre la stabilité du système financier dans son ensemble. L'exposition de l'écosystème des crypto-actifs à ce risque pourrait être exacerbée par ses spécificités techniques, notamment le recours aux blockchains, et l'introduction de nouveaux points de vulnérabilité tels que les ponts (bridges) entre les blockchains ou ce que l'on appelle les «oracles» qui alimentent les blockchains en données. À mon avis, la réussite de plusieurs cyberattaques visant des crypto-acteurs est un signal d'avertissement qui devrait attirer l'attention des régulateurs et des superviseurs. »

Un risque pointé par l'AMF, la manipulation des prix

Le régulateur français qu'est l'autorité des marchés financiers (AMF) a publié en juin 2023 un papier de discussions « Finance décentralisée (DeFi), protocoles d'échange et gouvernance : vue d'ensemble, tendances observées et points de discussion réglementaires ».

À l'aube de l'entrée en vigueur de MiCA, le régulateur, ayant également pour rôle d'aiguiller ses acteurs, n'a pas perdu de temps en soulevant des points d'approches réglementaires sur la DeFi. C'est notamment dans ce papier de discussion qu'il a déclaré :

« Une des limites découlant de ce modèle est que les protocoles d'échange DeFi ont tendance à s'appuyer sur l'utilisation d'informations externes, notamment pour déterminer les prix initiaux, car l'évaluation de la valeur d'une réserve suppose une connaissance préalable de la valeur des actifs qui s'y trouvent…

….Une telle dépendance se caractérise par l'utilisation de flux de données externes (pouvant provenir d'autres protocoles DeFi, mais parfois aussi depuis des plateformes CeFi) intégrés au smart contract du protocole. En DeFi, de telles sources sont appelées « oracles », et soulèvent un certain nombre de questions au regard des risques qu'elles engendrent. »

Comprenant bien le rôle des oracles, l'AMF reconnaît que les « oracles peuvent être utilisés pour corriger des divergences potentielles de valorisation des crypto-actifs au sein des protocoles d'échange DeFi »
mais « la source des données utilisées par certains oracles n'est pas toujours clairement communiquée et peut ainsi fausser les cours des actifs contenus dans les réserves de liquidité. […] Le recours à des oracles peut conduire à une manipulation potentielle des prix dans les protocoles, les données issues du marché cible de l'oracle – hors protocole – pouvant elles-mêmes être altérées. ».

Voici donc les deux principaux risques qui retiennent le point de vue des régulateurs. Ces craintes sont partagées à une échelle plus grande : l'échelle européenne.

Les pistes de réglementations européennes

La Task Force on Crypto-Assets and Decentralised Finance de l'organisme indépendant de l'Union européenne, le Comité européen du risque systémique (CERS) (en anglais European Systemic Risk Board, ESRB) a également publié un rapport sur les probables approches réglementaires de la DeFi.

Dans ce dernier, le risque dual (tant cyber que de manipulation du prix) rejoint le point de vue des régulateurs français soit que les oracles seront sujets à réglementation :

« *De plus, des exigences pour les oracles qui interagissent avec les smart contracts DeFi pourraient être nécessaires pour garantir qu'ils fonctionnent de manière robuste. »*

En outre, l'organisme de surveillance reprend les mêmes risques précédemment évoqués, mais énonce un catalyseur du risque : **la tokenisation des actifs du monde réel** (instruments financiers, droits de propriété etc) :

« Bien que les crypto-actifs soient encore largement auto-référentiels, il faut anticiper la tokenisation à grande échelle des actifs du monde réel. Si cela devait se produire, le système deviendrait beaucoup plus dépendant des oracles. Veiller à ce que le droit de propriété des actifs tokenisés soit enregistré sur blockchain privée, avec permission, atténuerait ce problème, car elle réduirait considérablement la possibilité d'exécutions automatisées du smart contract, à grande échelle, aux informations suspectes ou corrompues »

En plus du risque inhérent à la DeFi, ce dernier serait alors **amplifié du fait de la tokenisation à grande échelle des actifs** du monde réel qui, on le sait, est déjà en marche.

L'ESRB suggère simplement ici le recours aux blockchains privées, mais quelles sont les autres approches réglementaires proposées au sein de l'UE ?

Les Oracle services providers et la réglementation des Trust services providers

Déjà en 2018, un rapport « Comprendre les blockchains : fonctionnement et enjeux de ces nouvelles technologies » porté par des députés et sénateurs fut présenté devant le Sénat, expliquant les principaux rouages de la DeFi (mixers, nœuds, scalabilité, etc). Parmi eux est déjà mentionné le rôle des oracles :

« Par ailleurs, l'exécution de la plupart des cas d'usage annoncés, est conditionnée par l'apport et l'export d'informations. Que ce soit pour relever une température, livrer un colis, prouver la réalisation d'un travail, ou donner l'heure d'arrivée d'un avion, un tiers, qualifié d'« oracle » dans l'écosystème Ethereum, doit faire le lien entre la blockchain et le reste du monde, ce qui s'apparente au retour d'un « tiers de confiance » qui permet d'attester d'évènements au sein du monde réel, comme dans les exemples précédents. »

Il est intéressant ici de relever le terme employé pour définir les oracles : **des « tiers de confiance »**. Cette appellation est loin d'être anodine puisqu'elle désigne un prestataire réglementé qu'est le « prestataire de services de confiance » ou « trust services provider » ou plus simplement « TSP ».
Un tel statut est d'ores-et-déjà soumis au règlement européen du 23 juillet 2014 dit « eIDAS ». À l'heure actuelle, un tiers de confiance est donc, selon cet instrument juridique européen, une personne physique ou morale proposant des services **tels que la vérification ou la validation de signatures électroniques, de cachets électroniques, d'horodatages électroniques ou encore d'authentification sur un site web.**

Cette potentielle assimilation des Oracle Service Providers aux TSPs n'est pas seulement nationale.

Cette éventualité est partagée par un forum créé par la Commission européenne le « EU Blockchain Observatory and Forum ». Dans un rapport de ce dernier « Legal and regulatory framework of blockchains and smart contracts » de septembre 2019, un éventuel rapprochement de ce règlement eIDAS aux oracles est évoqué :

« Comme nous l'avons vu plus haut, pour être juridiquement valables en Europe sous eIDAS, les signatures numériques sur une blockchain doivent être vérifiées par un TSP. Un smart contract juridique exigeant de telles signatures numériques devra pouvoir vérifier si la signature est valide, si elle fait référence à la bonne personne et, si tel est le cas, si cette personne a réellement le pouvoir de signer.
Dans un contexte commercial, cela peut signifier pouvoir accéder aux bases de données de l'entreprise ou à un autre oracle fiable. Ceux-ci, à leur tour, auraient besoin d'une sorte de statut juridique. »

En outre, il n'est pas strictement dit ici qu'eIDAS sera appliqué aux oracles. Ce passage faisant d'avantage figure de piste de réglementation dédiée à ces derniers mais prenant comme inspiration un règlement européen effectif et existant depuis 2014.

Le rapport de la direction générale FISMA de la Commission européenne, au lendemain de MiCA

Le règlement MiCA n'a pas vocation à traiter de la DeFi. C'est à ce titre que le Conseil de l'Union Européenne, lors de sa communication de l'accord trouvé par les institutions européennes sur MiCA datant du 30 juin 2022, indique que dans les prochains mois la Commission européenne sera invitée à travailler sur une évaluation du marché des NFT et de la finance décentralisée pour in fine proposer une réglementation.

C'est dans ce contexte qu'il convient d'étudier le rapport d'octobre 2022 de la DG FISMA contenant des propositions de réglementations de la DeFi via les oracles. Ce document provient de l'une des 33 directions générales de la Commission européenne (qui n'est pas liée par ce rapport) à savoir la direction générale de la stabilité financière, des services financiers et de l'union des marchés des capitaux.

Il ne faudrait pas s'avancer mais si un MiCA 2 portant sur la DeFi voit le jour, il ne serait pas étonnant de voir une ou plusieurs dispositions s'inspirer de ce document.

Tout d'abord on y retrouve certes les mêmes risques mais surtout des propositions. Celles-ci ne sont pas simplement liées aux oracles mais à la régulation de la DeFi dans son ensemble en partant d'une réglementation sur ces derniers.

Plusieurs propositions sont établies :

- des oracles publiques
- des standards et lignes de conduites publiés par les régulateurs
- un statut juridique à part entière.

Oracles publiques :
La DG FISMA propose ici d'instaurer des critères de confiance à l'oracle. Afin qu'un protocole DeFi puisse l'utiliser sans inquiétude du superviseur, les données doivent être :

- vérifiables dans « l'économie réelle »
- publiques
- quantitatives/ mesurables (ou « hard »)
- à un prix qui n'est pas trop élevé (ici sont notamment entendues les frais)
- statiques

À titre de comparaison, le rapport prend l'exemple des bases de données recensant les défauts de paiement des États : les « sovereign defaults ».

Standards et lignes de conduites :
Le rapport propose ici une implication très restreinte des régulateurs dans la conformité des Oracle services providers en évoquant simplement un rôle de guide. A l'instar de régulateurs comme la CNIL qui formulent aux responsables de traitements de données personnelles des guides et recommandations de façon constante, les régulateurs publieraient régulièrement des lignes directrices, voire des standards spécifiques en fonction du type de données fournies par l'oracle.

La licence d'Oracle services provider:
Enfin, voici la proposition qui pourrait être la plus alléchante pour un régulateur : la création d'un statut juridique à part entière pour ces acteurs (comme évoqué dans la comparaison avec les TSP plus haut).

Cela permettrait aux victimes de manipulation de prix via l'oracle de se retourner plus rapidement vers la personne responsable, réclamer des dommages et intérêts, etc.

La proposition la plus marquante est celle permettant aux Oracle services providers dûment immatriculés de **délivrer des NFT non-négociables liés à des KYC.** Cela assure la confiance envers les données fournies et l'identité du fournisseur grâce au scoring lié.

Ainsi, pour les clients utilisant la DeFi, le NFT pourrait être directement identifié, renforçant le sentiment de confiance on-chain des données fournies par les Oracle services providers.
Cette possibilité de délivrance de NFT faisant office de certificats ferait alors de ces acteurs de véritables tiers de confiance de la DeFi et ce à l'instar des TSP.

AUX ÉTATS-UNIS

Le premier mot clé définissant l'approche des oracles au sein de la DeFi par un régulateur est encore et toujours le risque.

Ce dernier s'est concrétisé en octobre 2022 aux États-Unis à travers l'attaque de la plateforme Mango Markets par une manipulation d'oracle (nos confrères du JournalDuCoin en fait un résumé : hack de Mango Markets). Brièvement, l'attaquant en manipulant l'oracle a pu, à fortiori, manipuler les prix et repartir avec la somme de 112 millions de dollars.

Le hacker Avraham Eisenberg ou « Avi » a été arrêté par le FBI le 12 octobre 2022. Ce dernier fait désormais face à une action civile engagée par le régulateur américain des services portant sur les commodities, la Commodity Futures and Trading Commission (CTFC).

Le régulateur a lancé sa première action en justice basée sur une manipulation de marché attribuée à un oracle :

«This is the CFTC's first enforcement action for a fraudulent or manipulative scheme involving trading on a supposed decentralized dig ital asset platform, and its first involving a scheme that is sometimes called "oracle manipulation."»

De plus, dans cette communication publique, la CFTC y indique qu'elle est assistée dans son action par le régulateur en charge des services liés aux instruments financiers (autrement appelés « securities ») la Security and Exchange Commission ou « SEC ».
Cela ne s'arrête pas là ; les deux régulateurs ont été rejoints par le Department of Justice ou « DOJ » des États-Unis, l'équivalent américain du ministère de la justice français, dans une notification au juge en charge de l'affaire, dont le scellé a été levé le 27 décembre 2022.

Parmi les risques identifiés, on note les risques opérationnels, cyber, et bien entendu, ceux liés à la manipulation des prix. De plus, plusieurs recommandations y sont présentées:

- L'engagement de la responsabilité du provider lorsque celui-ci n'a pas effectué de due diligence sur la qualité des données fournies. Cela consiste à se reposer sur une unique source de données sans vérifier a minima s'il n'existe pas des données aberrantes dans ce qu'il récolte.
- Les pratiques et architectures de l'oracle doivent être transparentes.
- S'adapter à chaque protocole avec lequel il interagit.

Voir plus : le rapport énonçant les risques liés aux Oracles opérant dans la DeFi. de Greg Hopper de la Bank Policy Institute

Quels traits communs peut-on trouver dans ces approches pour essayer de deviner les contours de la régulation à venir de ces acteurs ?

Un régulateur des marchés financiers veut protéger ses investisseurs.

Pour cela, un acteur fautif doit être identifié, contrôlé et répondre de ses actes. En somme, avoir un statut juridique ad hoc qui a pour conséquence de lui conférer des obligations auxquelles il devra répondre devant un juge en cas de mauvaise action ou inexécution.

Un nouveau statut sera-t-il dédié à ces oracle services providers ou un existant leur sera appliqué ? L'avenir nous le dira.

Il est certain que, dans le nouveau comme le vieux continent, le minimum attendu d'un oracle services provider sera la transparence, la vigilance à l'égard des données fournies ainsi qu'une résilience informatique solide, humainement et matériellement.

Prêtresse de Delphes, John Collier, 1891

LES PERSPECTIVES

Le paysage technologique continuant de progresser à un rythme effréné, les oracles blockchain, autrefois considérés comme de simples intermédiaires, sont en passe de connaître une évolution, une spécialisation et une démocratisation remarquable.

Ils se préparent à revêtir des rôles plus spécifiques afin de répondre à des besoins sectoriels précis et démontrer des utilités tangibles dans divers domaines d'application.

La reconnaissance croissante de leur importance caractérise les prémisses d'une ère où les oracles ne sont plus de simples fournisseurs d'informations mais des acteurs majeurs du fonctionnement des écosystèmes blockchain.

Leur démocratisation promet de les rendre accessibles à une audience plus large. Cela permet ainsi à davantage d'applications et de services de bénéficier de la richesse et de la précision des données du monde réel intégrées dans les solutions décentralisées.

L'AVENIR DES ORACLES

Le marché des oracles blockchain se prépare à connaître une expansion majeure dans les prochaines années. L'adoption toujours croissante de la technologie blockchain à travers différents secteurs amplifie la demande d'intégration de données du monde réel de manière fiable et sécurisée au sein des réseaux blockchain.

D'après les études de marché, on prévoit une augmentation substantielle du marché mondial de la blockchain.

À l'heure actuelle, **le paysage des solutions oracle est dominé par Chainlink** qui a réussi à capturer une part impressionnante du marché. Cette prédominance soulève des interrogations quant aux acteurs qui pourraient potentiellement venir contester cette position dominante à court terme. Cependant, il est important de noter qu'une part de marché non négligeable demeure encore à la portée d'autres acteurs du domaine.

Cette fenêtre d'opportunité pourrait **attirer de nouveaux entrants ou encourager des acteurs existants** à innover et à proposer des solutions plus performantes ou différenciées pour gagner la confiance des utilisateurs et s'arroger une partie de cette part de marché encore disponible.

À titre d'exemple, certains protocoles se distinguent par leur efficacité et leur faible coût, notamment en matière de fourniture de prix ou de génération de nombres aléatoires (VRF).
Par exemple, RedStone offre des solutions oracle innovantes pour la DeFi actuelle en utilisant le stockage d'Arweave qui est bien moins cher de par son design.

Au lieu d'adopter l'approche des oracles traditionnels, RedStone stocke les données sur Arweave et les récupère à la demande via un réseau décentralisé.

Du côté du crédit, la technologie blockchain présente des opportunités sous-exploitées, particulièrement prometteuses pour la modernisation du secteur financier. **Les oracles de crédit**, qui facilitent l'évaluation financière et la solvabilité des entités au sein de la blockchain, sont anticipés pour connaître une croissance exponentielle. Ces mécanismes deviennent indispensables pour la maturation du secteur DeFi, en servant de pilier pour des services avancés tels que les mécanismes d'assurance et les dispositifs de recouvrement.

Toutefois, la mise en œuvre s'accompagne de défis considérables. Bien que des entités innovantes, telles que Spectral Finance, élaborent des solutions pour intégrer les systèmes traditionnels de notation de crédit à la blockchain, l'amalgame de ces deux univers n'est pas trivial. La grande interrogation réside dans la capacité d'intégrer ces données de manière cohérente, tout en garantissant transparence et sécurité optimales. En somme, si les oracles de crédit détiennent un potentiel considérable, une série d'obstacles techniques et réglementaires doit encore être adressée pour leur plein épanouissement.

Côté NFT, le marché a connu et connaît toujours une croissance rapide.
Selon un rapport de recherche approfondi de Market Research Future (MRFR), le marché devrait connaître une croissance significative pour atteindre une valorisation d'environ 342,54 milliards USD d'ici la fin de 2032.

Cette tendance entraîne une forte demande pour des données précises et fiables sur leur évaluation, leur popularité et les risques associés. Les informations extérieures comme la popularité d'un NFT, son historique de vente ou les interactions associées sur les réseaux sociaux, deviennent de plus en plus importantes à mesure que le secteur des NFT s'agrandit.

Banksea est une des plateformes conçue spécifiquement pour ce marché.
La plateforme intègre la big data et le Machine Learning pour fournir des évaluations précises.

Les oracles NFT se positionnent comme un élément incontournable pour enrichir et consolider le secteur. Ces oracles, dédiés à l'agrégation et à la fourniture de données externes aux blockchains, sont bien plus qu'un simple canal d'informations ; ils représentent une passerelle vers une meilleure compréhension et valorisation des NFT.

Cette incorporation de données extérieures contribue non seulement à une meilleure transparence du marché mais aussi à son évolution et à sa maturité.

Enfin, **les oracles d'identité**, ou "dID", redéfinissent la gestion des identités numériques via la blockchain, offrant une vérification sécurisée et transparente. Cette approche décentralisée augmente le contrôle des utilisateurs sur leurs données et renforce leur confidentialité. À l'intersection des mondes numérique et physique, les dID facilitent et simplifient l'authentification.

À mesure que le monde évolue vers une plus grande dépendance à l'égard des transactions et interactions numériques, l'importance des oracles d'identité ne peut qu'augmenter.

Leurs applications potentielles s'étendent bien au-delà des simples transactions financières pour englober des domaines tels que la santé, l'éducation, le vote électronique et bien d'autres.

Ces systèmes d'identification décentralisés permettront de **créer des interactions plus transparentes, sécurisées** et centrées sur l'utilisateur. En outre, face aux préoccupations grandissantes concernant la vie privée et la sécurité des données, l'adoption des oracles d'identité pourrait bien représenter une réponse adaptée aux défis futurs en matière d'identification numérique.

Apollon du Belvédère, copie romaine d'un original du ive siècle av. J.-C. de Léocharès, musée Pio-Clementino.

L'INTÉGRATION DE L'IA ET DE L'IOT

L'intégration de l'intelligence artificielle (IA) dans les oracles blockchain ouvre une nouvelle ère d'innovations dans le domaine de la technologie décentralisée. L'association de la puissance de l'IA ajoutée à la sécurité et la transparence de la blockchain permet de concevoir des systèmes plus autonomes, intelligents et réactifs.

Dans le secteur de la DeFi, un oracle doté d'IA pourrait, par exemple, analyser en temps réel les flux de marché, prédire les volatilités et ajuster automatiquement les paramètres d'un contrat intelligent pour minimiser les risques ou optimiser les rendements.

Dans le contexte des chaînes d'approvisionnement basées sur la blockchain, les oracles avec IA peuvent suivre en temps réel les mouvements de marchandises, prédire les retards ou les inefficacités grâce à l'analyse de données et intégrer ces informations directement dans la blockchain **pour assurer transparence et traçabilité**. Les décisions automatiques pour réacheminer les marchandises ou informer les parties prenantes peuvent alors être prises en se basant sur la blockchain, garantissant ainsi **une réduction des coûts et une amélioration significative de l'efficacité** des chaînes d'approvisionnement.

Dans le futur, avec l'évolution rapide des capacités de l'IA et l'adoption croissante de la blockchain, ces oracles "intelligents" deviendront probablement la norme dans de nombreux domaines d'application.

Du côté de l'IoT, à mesure que cette technologie progresse, la symbiose avec les oracles blockchain devient de plus en plus pertinente.

L'IoT repose sur **la capacité des appareils à communiquer entre eux** et à échanger des données en temps réel. Les oracles blockchain ont le potentiel d'ajouter une couche de sécurité et de vérifiabilité à ces échanges.

En effet, avec des milliards d'appareils connectés recueillant et transmettant des informations, la nécessité d'une source de données fiable et transparente est essentielle.

Le buste de Zeus découvert à Otricoli, en Italie.

L'ÉMERGENCE DES CASINOS WEB3

Avec l'arrivée de la régulation, beaucoup d'exchanges centralisés et décentralisés recontrent des barrières à l'entrée dans certains pays.

Même la décentralisation a ses limites ! Rappelons que certains DEX ont dû bloquer leur front-end pour les utilisateurs américains.

D'autre part, les exchanges centralisés comme Binance ont dû supprimer les produits à effet de levier pour tous les utilisateurs français.

Ces contraintes de régulation et le bear market ont fait émerger de nouvelles solutions : **les Casinos web3**.
Ces plateformes proposent tous les moyens possibles de perdre votre argent : des paris sportifs, des jeux classiques type roulette et blackjack automatisés ainsi que des paris à effet de levier sur la direction des différentes cryptomonnaies allant jusqu'à x1000.

Rollbit, le casino populaire des amateurs crypto, enregistre plusieurs millions de dollars de revenus journaliers. Sur ces revenus, 30% servent à racheter le token natif de la plateforme ($RLB) afin de le burn, gonflant ainsi la demande et le prix du token.

Aujourd'hui, la majorité des casinos en ligne n'a pas été conçue nativement pour le Web3. Cela signifie qu'avant de jouer sur ces plateformes, il vous faut transférer vos fonds vers l'adresse fournie par le casino. Cette étape est souvent nécessaire en raison des frais associés et de la complexité de placer des paris directement depuis un portefeuille électronique.

Toutefois, avec l'arrivée des solutions Layer 2 sur Ethereum et l'évolution vers des blockchains toujours plus rapides et efficaces, on peut anticiper l'apparition de casinos natifs du Web3. Ces nouveaux casinos promettent plus de transparence grâce à l'utilisation de smart contracts vérifiables et un recours accru aux données.

En consultant les documents sur le site de Rollbit, nous voyons aujourd'hui que le prix des cryptomonnaies de la plateforme est récupéré directement sur les exchanges centralisés comme Binance, Huobi, OKEx ou encore Kraken ou Coinbase.

Selon nous, les casinos qui nécessitent des données fiables, transparentes et accessibles en permanence pourraient être une grande opportunité pour les oracles qui ont encore du mal à établir ***un modèle économique rentable sans l'utilisation de tokens***.

De plus, le besoin des VRF, abordés plus tôt dans ce dossier, pourrait également représenter une grande opportunité pour les oracles.

Statue en marbre de la déesse Cybèle, ier siècle av. J.-C. (Formia, Latium).

LE MOT DE LA FIN

Les oracles blockchain sont devenus incontournables dans le paysage technologique actuel, jouant un rôle crucial dans des domaines aussi variés que la DeFi, les jeux Web3, les NFT et bien plus encore.

Ces intermédiaires, **qui connectent le monde réel et les différents protocoles à la blockchain**, sont non seulement indispensables pour intégrer des informations fiables et sécurisées mais aussi pour renforcer l'intégrité des transactions dans ces domaines.

L'avenir des oracles est étroitement lié à la croissance et à l'évolution du secteur blockchain.

Avec l'émergence d'oracles spécialisés dans des domaines tels que l'identification numérique décentralisée (dID), les NFT, le crédit et d'autres, on peut s'attendre à voir ces solutions prendre une place prépondérante lors du prochain bull run.

Parallèlement, l'intégration des oracles avec des technologies de pointe comme l'intelligence artificielle (IA) et l'Internet des objets (IoT) **ouvre la voie à des innovations inédites** où les oracles ne sont pas simplement des ponts d'information mais des catalyseurs pour des systèmes plus autonomes, réactifs et intelligents.

Face à cette croissance et à l'innovation effrénée, le marché des oracles est destiné à se diversifier, donnant lieu à des solutions spécialisées qui répondront aux besoins uniques de différents secteurs.

Que ce soit par l'analyse des flux du marché en temps réel, la garantie de la traçabilité des produits ou la création de systèmes d'identification transparents, les oracles continueront **d'évoluer et de façonner l'avenir de la technologie blockchain**, rendant les processus plus transparents, sécurisés et centrés sur les besoins des utilisateurs.

Les oracles blockchain font encore face à de nombreux défis aujourd'hui
Sur le plan interne, ils doivent gérer la concurrence, surmonter les bugs techniques et identifier des sources de revenus stables sans se reposer sur la vente de tokens.
Sur le plan externe, ils sont confrontés aux enjeux de régulation, à la quête de reconnaissance et d'adoption par les institutions financières traditionnelles ainsi qu'à l'émergence de protocoles qui fonctionnent sans nécessiter d'oracle.

Une certitude demeure ; quiconque s'intéresse aux cryptomonnaies et à la blockchain devrait **garder un œil attentif sur l'évolution du secteur des oracles.**

La Sibylle de Delphes, fresque de Michel-Ange (1508–1512).

REMERCIEMENTS

Nous souhaitons exprimer notre gratitude envers tous ceux qui ont pris le temps de lire ce dossier et de le partager.

Votre intérêt et votre soutien nous encouragent à mener à bien ce type de travail de recherche complexe et ambitieux.

Aussi, nous tenons à remercier toutes les personnes qui ont contribué à ce dossier :

Enguerrand Denoual, juriste spécialisé en droit des crypto-actifs, pour l'écriture de la partie Réglementation.

Mathilde Jenot, Ottavia Lampe, Clément Aguillé (Meria) et Erwan Gallo pour leur travail de relecture.

Pyth Network pour avoir rendu l'écriture de ce dossier possible.

"Sans les oracles, la DeFi n'existerait pas. Garantir l'exactitude, la fiabilité et la disponibilité des données est d'une importance primordiale pour que les oracles servent correctement ce secteur. Le réseau Pyth a été conçu dès le départ pour résoudre les problèmes des oracles traditionnels. Les innovations de Pyth incluent des fournisseurs de données "first-party", une conception d'oracle à faible latence, un catalogue de flux de prix inégalé et une connexion à plus de 35 blockchains." - ***Marc Tillement, Directeur, Pyth Data Association***

DISCLAIMER

Les personnes ayant rédigé ce dossier possèdent des cryptomonnaies, y compris certains actifs mentionnés dans le texte.

Le contenu de ce dossier est fourni à titre informatif et uniquement à des fins éducatives. Il est gratuit et accessible à tous. Ce dossier ne constitue en aucun cas un conseil financier ou une incitation à investir dans les cryptomonnaies ou tout autre actif financier.

L'investissement implique des risques financiers importants, dont la perte totale ou partielle du capital. Ce placement peut s'avérer hautement spéculatif et volatile. Il est important de prendre les dispositions personnelles nécessaires avant de placer son argent dans n'importe quel domaine financier.

Les auteurs ne seront pas responsables des pertes ou des dommages directs ou indirects résultant de l'utilisation ou de la confiance accordée à ce dossier de recherche ou à son contenu.

Enfin, il est à noter que la mention de noms de cryptomonnaies dans ce dossier de recherche ne constitue pas une recommandation ou une approbation de ces actifs par l'auteur ou toute entreprise ou organisation mentionnée dans ce document.

Ce dossier a été réalisé grâce au soutien financier de Pyth Network.

Cependant, comme précisé dans la déontologie de rédaction, notre sponsor n'a eu aucun droit de regard sur le contenu dossier.

Tout contenu rédigé et présenté a été réalisé à des fins éducatives et de façon complètement impartiale.

LEXIQUE

- Oracle: Entité ou protocole qui fournit des données extérieures à une blockchain, permettant ainsi aux contrats intelligents de traiter des informations ne provenant pas originellement de la blockchain.
- Web3: Terme décrivant une nouvelle génération d'applications sur le web, utilisant les technologies de la blockchain et des contrats intelligents.
- Contrat intelligent (Smart Contract): Script auto-exécutable stocké sur une blockchain, qui s'exécute lorsque des conditions pré-définies sont remplies.
- Décentralisation: Distribution des pouvoirs et ressources à travers un réseau, sans point central de contrôle.
- Source de données: Origine des informations que l'oracle va récupérer. Peut être une API, une base de données, etc.
- Fiabilité: Capacité d'un oracle à fournir des informations précises et non altérées.
- Chainlink: L'une des principales plateformes d'oracle décentralisées.
- Prophétie (Fetch): Acte de récupérer une information via un oracle.
- Node (Nœud): Serveur ou ordinateur sur lequel un oracle fonctionne.
- Feed de prix: Flux de données fournissant les prix actuels d'actifs spécifiques, comme les cryptomonnaies.
- API: Interface de programmation permettant l'accès à des informations ou des fonctionnalités d'une autre application.
- Consensus: Accord parmi un groupe de parties pour valider une information ou une transaction.
- Token ERC-20: Standard pour les jetons sur Ethereum, souvent utilisé pour les cryptomonnaies et d'autres actifs numériques.
- Sécurité économique: L'idée que le coût de l'attaque d'un système est supérieur au gain potentiel.
- Données off-chain: Informations qui ne résident pas sur la blockchain mais peuvent être accessibles par elle.
- Middleware: Logiciel servant d'intermédiaire entre différentes applications, comme entre un contrat intelligent et une source de données.
- Attaque Sybil: Attaque où une seule entité contrôle plusieurs nœuds dans un réseau, faussant le mécanisme de consensus.
- Réseau test (Testnet): Version alternative de la blockchain utilisée pour les tests.
- Band Protocol: Une autre plateforme d'oracle décentralisée en concurrence avec Chainlink.
- Tiers de confiance: Entité ou système en qui les utilisateurs placent leur confiance pour valider des informations ou des transactions.

LEXIQUE

- Validation: Processus de vérification de l'exactitude et de la fiabilité des données.
- Oracles décentralisés: Oracles qui fonctionnent sur plusieurs nœuds pour assurer la fiabilité et réduire la centralisation.
- Staking: Acte de mettre en gage des tokens comme garantie pour certaines actions, souvent utilisé pour encourager l'honnêteté dans les systèmes d'oracles.
- Attaque à 51%: Scénario où une entité contrôle plus de 50% de la puissance de calcul, compromettant la sécurité du réseau.
- Oracles réputés: Oracles qui ont gagné la confiance des utilisateurs grâce à leur historique d'exactitude et de fiabilité.
- Endossement: Validation ou approbation par des parties tierces.
- Latence: Délai entre la demande d'information et sa réception.
- Mise à jour: Acte d'intégrer les nouvelles données ou informations dans un système.
- Oracles hardware: Dispositifs physiques qui recueillent et transmettent des données à la blockchain.
- Oracles logiciels: Oracles qui fonctionnent entièrement en ligne et recueillent des données de sources numériques.
- Oracles de consensus: Oracles basés sur l'accord de plusieurs parties pour valider une donnée.
- Oracles de majorité: Oracles qui déterminent la véracité d'une donnée basée sur la majorité des retours.
- Oracle de marché: Oracle qui utilise les mécanismes de marché, comme l'offre et la demande, pour fournir des données.
- Vérification de l'oracle: Processus de s'assurer qu'un oracle fournit des données précises.
- Données on-chain: Informations résidant directement sur la blockchain.
- Adaptateur: Logiciel qui traduit les demandes de données entre les contrats intelligents et les sources de données extérieures.
- Oracles incitatifs: Oracles qui récompensent les fournisseurs de données précises et pénalisent les données inexactes.
- Réseau principal (Mainnet): La version principale et opérationnelle d'une blockchain.
- Gas: Frais payés pour les transactions et les contrats intelligents sur les réseaux blockchain comme Ethereum.
- Synchronisation: Processus de mise à jour des nœuds pour qu'ils aient la même information.

LEXIQUE

- DAO (Organisation Autonome Décentralisée): Structure organisée de manière décentralisée sans une autorité centrale, souvent basée sur des contrats intelligents.
- Oracles en cascade: Système où un oracle consulte plusieurs autres oracles pour obtenir une moyenne ou un consensus.
- Oracles manuels: Oracles gérés par des humains qui entrent manuellement des données.
- Oracles automatiques: Oracles qui fonctionnent sans intervention humaine.
- Souscription: Contrat entre un oracle et un utilisateur spécifiant les détails de la fourniture de données.
- Mise à l'échelle: Augmentation de la capacité d'un réseau ou d'un système.
- Cryptographie: Science de la sécurisation des informations à travers le codage.
- Vérification en chaîne: Vérification des données directement sur la blockchain.
- Vérification hors chaîne: Vérification des données en dehors de la blockchain.
- Redondance: Duplication de certaines parties du système pour assurer la continuité en cas de défaillance.
- Multi-sig (Multisignature): Un mécanisme de sécurité où plusieurs signatures sont requises pour valider une transaction.
- Gouvernance décentralisée: Mécanisme par lequel les décisions concernant un réseau ou un protocole sont prises collectivement par ses participants plutôt que par une entité centrale.
- Ponts (Bridges): Solutions qui connectent différentes blockchains, permettant l'échange d'informations et de valeurs entre elles.
- Slashing: Pénalité appliquée à des participants malveillants ou non performants dans un réseau décentralisé. Dans le contexte des oracles, cela pourrait signifier la perte de tokens mis en gage pour fournir des données incorrectes.
- Whitelisting: Processus d'autorisation où seules les entités approuvées peuvent participer ou accéder à certaines fonctions.
- Zéro connaissance (Zero-knowledge proofs): Méthodes cryptographiques qui permettent à une partie de prouver à une autre qu'une déclaration est vraie sans révéler d'autres informations. Utile pour la confidentialité et la sécurité dans l'espace blockchain.

OAKINVEST

SPONSORISÉ PAR PYTH