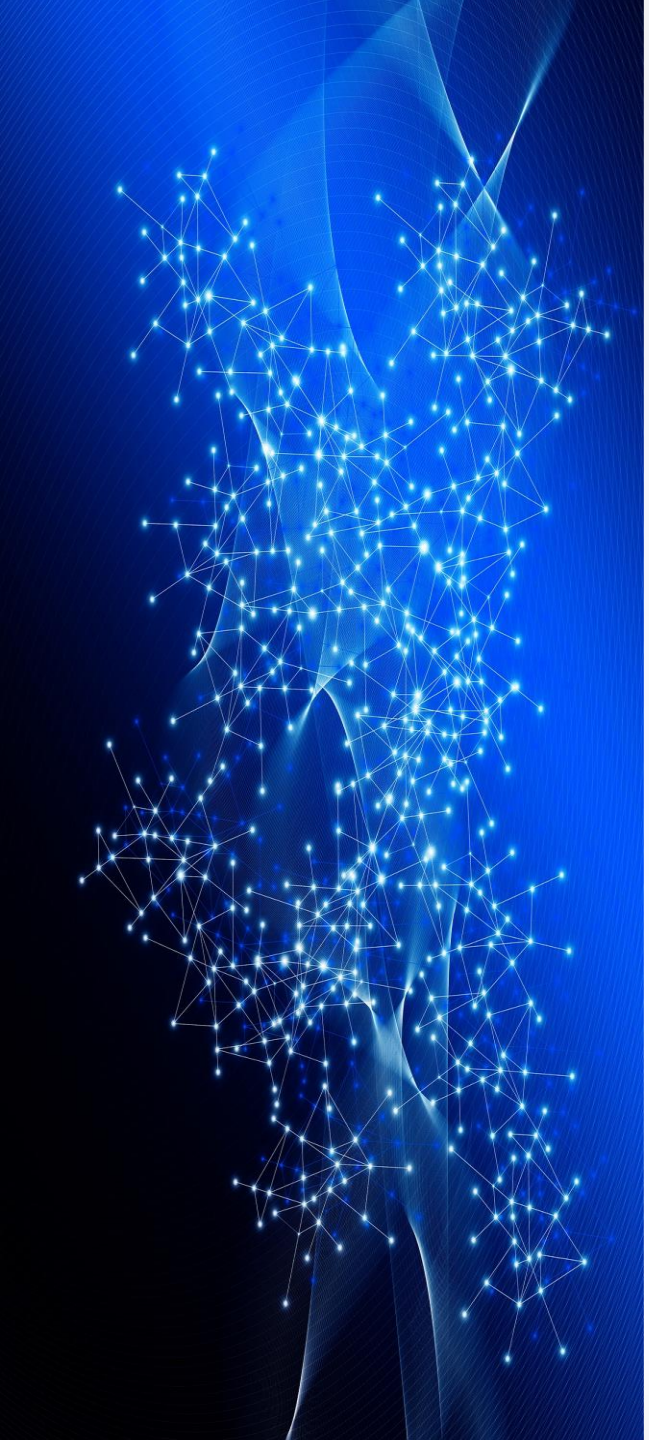

université virtuelle Burkina Faso

Introduction a la programmation blockchain

Professeur

Mr. Amon M. R. BAZONGO

université virtuelle Burkina Faso

Intégration de Contrats Intelligents avec des Oracles : Exploration des scénarios d'utilisation des oracles pour connecter des contrats intelligents à des sources de données externes

université virtuelle Burkina Faso

Participants

- BADOLO Micheline Latifatou
- FOFANA Abdoul-rachid B.
- SOME Wend Bele Diane

université virtuelle Burkina Faso

Sommaire

Sommaire

Introduction

Introduction

Au cœur de la blockchain et des contrats intelligents, les oracles émergent comme des facilitateurs critiques, connectant le numérique au monde réel. Explorez avec nous comment ces oracles rehaussent l'efficacité et la confiance dans divers scénarios d'utilisation.

Les contrats intelligents et les oracles

Les contrats intelligents et les oracles - les contrats intelligents

Un contrat intelligent est un protocole informatique qui facilite, vérifie et exécute la négociation ou l'exécution d'un contrat, ou qui rend une clause contractuelle inutile (car rattachée au contrat intelligent) . Les contrats intelligents sont du code informatique qui émule la logique des clauses contractuelles. Ils ont généralement une interface utilisateur et peuvent être utilisés pour automatiser des processus de négociation ou d'exécution de contrats.

Les contrats intelligents et les oracles - les oracles

Un oracle est un dispositif qui fournit des données à un contrat intelligent . Les oracles peuvent être centralisés ou décentralisés. Les oracles centralisés sont contrôlés par une entité unique fournissant des données à un contrat intelligent. Les oracles décentralisés, en revanche, interagissent avec plusieurs sources de données, sans être contrôlés par une seule entité . Les oracles sont utilisés pour fournir des données externes à un contrat intelligent, telles que des informations sur les prix des actifs, des données météorologiques et bien d'autres de la vie courante.

Les contrats intelligents et les oracles - limites et avantages

Les contrats intelligents et les oracles ont des avantages et des inconvénients. Les avantages des contrats intelligents sont qu'ils sont numériques et automatisés, ce qui signifie qu'aucun traitement de document papier n'a lieu et aucun temps n'est consacré à rectifier les erreurs qui résultent généralement du remplissage manuel des documents. Comme aucun tiers n'est impliqué et que les enregistrements chiffrés des transactions sont partagés entre les participants, la question de la modification des informations à des fins personnelles ne se pose pas. Les enregistrements de transaction dans la blockchain sont chiffrés, ce qui les rend pratiquement impossibles à détourner.

Les contrats intelligents et les oracles - limites et avantages

De plus, comme chaque enregistrement est relié aux enregistrements précédents et suivants dans un grand livre distribué, les pirates devraient modifier toute la chaîne pour changer un seul enregistrement. Les inconvénients des contrats intelligents sont qu'ils sont encore relativement nouveaux et que leur adoption est limitée. Les contrats intelligents sont également limités par la capacité de la blockchain à traiter les transactions .

université virtuelle Burkina Faso

Les contrats intelligents et les oracles - limites et avantages

Les avantages des oracles sont qu'ils permettent aux contrats intelligents d'interagir avec le monde extérieur, ce qui est essentiel pour de nombreux cas d'utilisation. Les inconvénients des oracles sont qu'ils sont vulnérables aux attaques et qu'ils peuvent être coûteux à utiliser .

Scénarios d'utilisations et leurs avantages

Scénarios d'utilisations - Finance Décentralisée (DeFi)

La finance décentralisée, ou DeFi, révolutionne la manière dont les services financiers sont fournis en éliminant les intermédiaires traditionnels. L'intégration d'oracles dans les contrats intelligents offre des avantages significatifs pour divers aspects de la DeFi. Dans le cadre des prêts et des emprunts, les oracles peuvent fournir des données en temps réel sur les taux d'intérêt, les prix des actifs et les garanties, permettant aux contrats intelligents de prendre des décisions autonomes basées sur des informations financières actualisées.

Scénarios d'utilisations - Finance Décentralisée (DeFi)

Cela représente des avantages tels que:
l’actualisation en Temps Réel : Les taux d'intérêt et les prix des actifs sont constamment mis à jour, permettant une prise de décision plus précise.
l’automatisation des Prêts : Les contrats peuvent automatiser le processus de prêt, éliminant ainsi le besoin d'intermédiaires.

Scénarios d'utilisations - Événements Sportifs et Paris Décentralisés

Les paris décentralisés exploitent la transparence et l'automatisation des contrats intelligents. Les oracles sont essentiels pour fournir des informations précises sur les événements sportifs.
Dans le cadre des paris décentralisés, les oracles peuvent fournir des résultats sportifs en temps réel, permettant aux contrats intelligents de distribuer automatiquement les gains aux participants.
Comme avantages il y’a :
la transparence : Les résultats des événements sportifs sont vérifiables et transparents grâce aux données fournies par les oracles.
l’automatisation des Paiements : Les gains sont distribués automatiquement sans besoin d'une tierce partie.

Scénarios d'utilisations - Contrats d'Options Programmables

Les contrats d'options programmables permettent la création de contrats financiers sophistiqués. L'intégration d'oracles offre des données externes pour informer ces contrats.
Dans le cadre d'options financières, les oracles peuvent fournir des informations sur les prix d'actifs sous-jacents, permettant aux contrats intelligents d'exécuter automatiquement des options en fonction de ces données.

Scénarios d'utilisations - Contrats d'Options Programmables

Nous relevons des avantages comme :
l’exécution autonome : Les contrats d'options peuvent s'exécuter automatiquement en fonction des conditions du marché fournies par les oracles.
la réduction des risques : Les informations en temps réel réduisent les risques liés aux fluctuations du marché.

Scénarios d'utilisations - Vérification d'Identité

La vérification d'identité décentralisée gagne en popularité pour son approche sécurisée et privée. Les oracles jouent un rôle crucial en fournissant des données d'identité fiables.
Lors de la vérification d'identité, les oracles peuvent fournir des données de vérification, telles que des informations biométriques ou des vérifications de crédit, permettant aux contrats intelligents de prendre des décisions basées sur ces données.

Scénarios d'utilisations - Vérification d'Identité

Parmi ses avantages il y’a :
la sécurité des Données : Les données d'identité sont sécurisées et vérifiables grâce à des sources fiables fournies par les oracles.
l’automatisation des Processus : Les processus de vérification d'identité peuvent être automatisés sans compromettre la sécurité.

Intégration des Oracles aux Contrats Intelligents

Intégration des Oracles aux Contrats Intelligents - Processus

Le processus d'integration se déroule en plusieurs que sont:

Phase 1: Planification et Recherche

Objectifs : Définir clairement les besoins, les fonctionnalités et les sources de données externes nécessaires.

Phase 2: Développement du contrat intelligent

Objectifs : Créer et déployer le contrat intelligent de base.

Phase 3: Configuration et Déploiement du contrat oracle

Objectifs : Configurer et déployer le contrat oracle.

Intégration des Oracles aux Contrats Intelligents - Processus

Phase 4: Intégration et Tests
Objectifs : Connecter le smart contract à l'oracle et tester l'ensemble du système.

Phase 5: Déploiement sur le Mainnet
Objectifs : Déployer le contrat intelligent et le contrat Oracle sur le réseau principal Ethereum.

Intégration des Oracles aux Contrats Intelligents – Cas pratique

Prenons un exemple concret en utilisant Solidity pour créer un contrat intelligent pour la blockchain Ethereum. Dans cet exemple, nous allons utiliser le service Oracle de Chainlink pour récupérer le prix de l'ETH/USD. Pour se faire, il faut tout d'abord importer l'API de Chainlink dans le contrat intelligent avec cette ligne de code:

```
import "@chainlink/contracts/src/v0.8/interfaces/AggregatorV3Interface.sol";
```

Par la suite on écrit le contrat intelligent comme suit:

Intégration des Oracles aux Contrats Intelligents – Cas pratique

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.19;

contract MonContratIntelligent {
    // Adresse de l'oracle Chainlink pour l'ETH/USD
    address private oracle = 0x5f4eC3Df9cbd43714FE2740f5E3616155c5b8419;

    // Instance de l'interface de l'oracle
    AggregatorV3Interface internal priceFeed;

    // Constructeur
    constructor() {
        priceFeed = AggregatorV3Interface(oracle);
    }

    // Fonction pour récupérer le prix de l'ETH/USD
    function getEthUsdPrice() public view returns (int) {
        (
            uint80 roundID,
            int price,
            uint startedAt,
            uint timeStamp,
            uint80 answeredInRound
        ) = priceFeed.latestRoundData();

        return price;
    }
}
```

Enjeux et défis

Enjeux et défis - Sécurité et Gestion des Données

La sécurité est une pierre angulaire dans l'intégration des oracles, où la gestion des données doit concilier transparence et protection.
Cependant, les oracles, en tant que passerelles, peuvent être ciblés. Des failles pourraient compromettre l'intégrité des contrats intelligents.
Ainsi, la mise en place de protocoles robustes entre oracles et contrats intelligents est cruciale pour prévenir les attaques.
Aussi, la transparence de la blockchain peut exposer des données sensibles transitant par les oracles. Cela nécessite donc l'application de mécanismes de chiffrement avancés pour préserver la confidentialité des données transitant par les oracles.

Enjeux et défis - Coûts et Fiabilité des Oracles

L'économie des oracles crée des tensions entre coûts élevés et exigences de fiabilité, influant directement sur la confiance dans les contrats intelligents. Ainsi l'utilisation des oracles entraînant des dépenses significatives, notamment dans des secteurs nécessitant une actualisation fréquente des données, la recherche de moyens de réduction des coûts est impérative.

De plus, la dépendance aux oracles externes suscite des inquiétudes quant à leur fiabilité, engendrant des erreurs potentielles dans l'exécution des contrats. Ainsi, pour garantir la fiabilité optimale dans la transmission des données, l'établissement de critères stricts de sélection des oracles est nécessaire.

Enjeux et défis - Adoption et Normalisation

L'adoption généralisée des oracles et la standardisation des protocoles sont des obstacles qui influent sur la maturité et l'acceptation de cette technologie.
Ainsi, l'absence de normes communes peut créer une fragmentation des protocoles d'oracle, rendant l'interopérabilité complexe.
De plus, certains secteurs peuvent hésiter à adopter des contrats intelligents dépendant d'oracles en raison de préoccupations liées à la fiabilité et à la sécurité.

Conclusion

Conclusion

L'intégration des oracles dans les contrats intelligents offre des avantages substantiels, mais n'est pas sans défis. Les enjeux de sécurité, les coûts élevés et les défis d'adoption nécessitent une approche équilibrée. Un engagement continu dans la recherche, le développement de normes et la sensibilisation sont essentiels pour surmonter ces obstacles et libérer le plein potentiel des oracles dans les contrats intelligents.

Merci de nous avoir accordé votre intérêt!