Blockchain CheatSheet - La Vision

Temps de lecture : 9 min

Table des Matières

- Le Mécanisme du Fork
- Leçons

§ Blockchains Privées

- Cas d'utilisation Spécial

§ Les Propriétés de la Vision Blockchain

- Risques des Cryptomonnaies

§ Bitcoin

Aperçu

Une base de données distribuée en pair-à-pair comme un grand livre public qui prouve la propriété
Aucune confiance nécessaire Les fonctionnalités des blocs et la propriété sont enregistrées dans l'historique immuable de la chaîne (les livres).
Sécurité et Efficacité soutenues par une cryptographie solide et le réseau de ordinateurs le plus puissant
Les mineurs fournissent la sécurité par le biais d'un système de récompense

Hashing

Les blocs de la blockchain Bitcoin sont, par conception, composés de données de 10 minutes chacun, une pratique établie depuis 2009.

Caractéristique de la chaîne:

- Chaque dernière ligne (hash) d'un bloc est un hash SHA-256 des données du bloc.
- Ce hash devient la première ligne du bloc suivant.
- Si vous modifiez un bloc, son hash SHA-256 changera également.
- Ce changement rompra la chaîne car la première ligne du bloc suivant ne correspondra plus.

Mining en Proof of Work

- **But** : Assurer l'immuabilité de la blockchain.
- **Comment cela se fait** : Des *nonces* (Nombres Utilisés Une Seule Fois) sont ajoutés à la fin du hash de chaque bloc pour trouver un hash ayant un certain nombre de zéros en tête, validant ainsi le bloc.
- **Pourquoi** : Le système nécessite une preuve que du travail computationnel a été effectué. Trouver un hash avec un certain nombre de zéros en tête est difficile et nécessite de nombreuses tentatives, démontrant ainsi que du travail a été réalisé.
- **Sécurité** : Ce processus rend difficile pour quiconque de modifier les données sans refaire tout le travail computationnel, renforçant ainsi la sécurité de la blockchain.

§ Ethereum et Blockchains Nouvelle Génération

Enfant et Amélioration de la Blockchain Bitcoin

Aujourd'hui, Ethereum se présente comme l'une des technologies les plus, sinon la plus, importante pour les applications commerciales. Il conserve toutes les fonctionnalités de Bitcoin tout en offrant la possibilité d'incorporer des petites applications au sein des blocs. Cela nous permet de construire un système informatique décentralisé en utilisant la structure de la blockchain. De plus, il élargit la gamme de données pouvant être utilisées sur la blockchain, et avec la technologie des contrats intelligents, il améliore encore les capacités de transaction.

Quelques dénominations de dimensions

- **Wei** : Multiplicateur 10^0
- **Szabo** : Multiplicateur 10^{12}
- **Finney** : Multiplicateur 10^{15}
- **Ether** : Multiplicateur 10^{18}

Concept des Contrats Intelligents

- **Mises à jour d'état programmatiques**
  - Peut ajouter toute fonctionnalité désirée.
- **Peut faciliter l'accès et la distribution de fonds basés sur des conditions spécifiées**
- **Peut créer, transférer et modifier des actifs numériques arbitraires**
- **Interagit avec d'autres contrats pour créer des applications robustes et interopérables**
- **Base pour l'Internet de la Valeur**

Applications Décentralisées (dApps)

Comme mentionné précédemment, Ethereum et d'autres blockchains nouvelle génération offrent la possibilité de développer des Applications Décentralisées (dApps). Ces applications utilisent une série de technologies telles que les contrats intelligents pour la logique des applications, IPFS ou Swarm pour le stockage des données, les Services de Noms Ethereum (**ENS**) pour la dénomination de domaine décentralisée, et Whisper pour la messagerie décentralisée entre applications.

Explication

- **Ethereum et Blockchains Nouvelle Génération** : Ces plateformes soutiennent le développement de dApps, permettant des solutions innovantes et décentralisées.
- **Contrats Intelligents** : Utilisés pour implémenter la logique et les règles des dApps.
- **IPFS ou Swarm** : Solutions de stockage décentralisées pour stocker et récupérer des données.
- **Services de Noms Ethereum (ENS)** : Fournit un DNS décentralisé pour des noms faciles à lire.
- **Whisper** : Un protocole pour la messagerie décentralisée, permettant une communication sécurisée entre dApps.

Contexte

- **Applications Décentralisées (dApps)** : Applications qui fonctionnent sur un réseau décentralisé, utilisant la technologie blockchain pour assurer sécurité, transparence et fiabilité.

> En fin de compte, il est sage de considérer Ethereum comme la première idée révolutionnaire et brillante qui a conduit à la création de la couche fondamentale pour l'Internet de la Valeur et les applications décentralisées.

---

§ Stockage

Types de Comptes

Comptes Détenus Externement (EOA)

- Compte géré par des humains
- Système de clés publiques et privées pour gérer les transactions

Comptes de Contrats

- Comptes avec code incorporé, gérés une fois déployés
- Peuvent détenir et transférer BTC, ETH ou d'autres Tokens
- Inchangeable en dehors de ce qui est codé

Portefeuilles

Définition : Un outil composé d'un ou plusieurs comptes utilisés pour stocker et transférer BTC, ETH ou d'autres tokens.

Multisig : Divise vos clés pour améliorer la sécurité en nécessitant plusieurs signatures pour autoriser une transaction

§ Cryptomonnaies

Première Génération/Gold 2.0:

- **Bitcoin (BTC)** : La blockchain mère est limitée, tout comme **Litecoin (LTC)**.

Tokens de Computation Distribuée:

- **Ethereum (ETH)** : Révolutionne l'industrie en permettant à de petites applications de fonctionner sur le système blockchain. D'autres projets dans cette catégorie incluent **Tezos (XTZ)**, **EOS**, et **DFinity**.

Tokens

Contrairement aux pièces, qui ont leurs propres blockchains dédiées, les tokens existent sur et dépendent de la blockchain spécifique sur laquelle ils sont créés.

Tokens d'Utilité:

- Utilisés avec des actifs blockchain programmables, tels que **Storj**, **Golem (GNT)**, **Sia (SC)**, et **FileCoin**.

Tokens de Sécurité:

- Représentent des actions, obligations ou autres actifs, permettant aux tokens d'être utilisés à ces fins.

Tokens Fongibles:

- **ERC-20 token de la blockchain Ethereum** : Un protocole qui peut lier quelque chose à un token spécifique comme actif à référencer sur la blockchain Ethereum.

Tokens Non-Fongibles (NFTs):

- **ERC-721 token de la blockchain Ethereum** : Un protocole qui attribue de la valeur à une entité en utilisant un nouveau token unique, comme dans l'art.

Stablecoins:

- **Fiat Collatéralisé** : Indexé sur la valeur des monnaies fiat comme **EURC** ou **USDT**.
- **Cryptofiat National** : Tel que **Eurocoin** ou **Fedcoin**.
- **Collatéralisé par Actifs Naturels** : Tel que **Digix Gold (DGX)** ou **Swiss Real Coin (SRC)**.
- **Non-Collatéralisé** : Tel que **Basecoin**.

Ces, pour les esprits les plus entreprenants, sont susceptibles d'être le substitut ultime aux monnaies fiat.

---

§ Gaz

Le Problème

Le développement d'applications en chaîne pourrait entraîner des algorithmes défectueux, ce qui pourrait finir par consommer et gaspiller la puissance de calcul du système de nœuds de la blockchain.

Solution

Introduire des frais de "gaz" permet l'utilisation des applications et des contrats intelligents. C'est équivalent aux frais de transaction dans les blockchains Bitcoin, récompensant les mineurs pour la gestion de la puissance de calcul des applications dans une certaine mesure, déterminée par le montant de gaz.

Analogie

Avoir une voiture avec une pédale d'accélérateur défectueuse pourrait être dangereux avec du gaz infini. C'est l'idée mise en œuvre dans la blockchain : elle limite l'utilisation des applications par le montant de frais de gaz que vous êtes prêt à dépenser.

---

§ The DAO (Organisation Autonome Décentralisée)

Un DAO (Organisation Autonome Décentralisée) est une organisation construite par le biais de contrats intelligents financés par des investisseurs qui reçoivent des tokens pour voter. À l'époque, les tokens DAO représentaient une partie significative de la valeur marchande d'Ethereum et étaient considérés comme des valeurs mobilières en raison de leur valeur en tant que tokens de décision dans une structure d'entreprise.

Un Problème est survenu

Un bug a été découvert permettant des retraits illimités sans comptabilité appropriée, drainant les réserves. C'était un problème majeur.

Les Dommages et La Fortune

Les contrats intelligents DAO ont été piratés en deux tentatives, l'une retirant 30% et l'autre 70% de la valeur du projet simultanément. Heureusement, le contrat intelligent était codé avec une période de règlement de 28 jours.

La Résolution

La communauté a choisi ensemble de faire un hard fork de la blockchain, réécrivant son histoire pour éviter cet incident, retournant les tokens sous forme d'ETC (Ethereum Classic) aux propriétaires d'origine.

Le Mécanisme du Fork

Tout comme une nouvelle version d'un système d'exploitation peut gérer une ancienne version d'Excel, un Soft Fork est un type de mise à jour qui introduit de nouvelles règles compatibles avec les versions antérieures. C'est similaire à la manière dont Microsoft Windows peut être mis à jour pour supporter de nouvelles fonctionnalités tout en exécutant des applications plus anciennes.

En revanche, si vous mettez à niveau vers de nouvelles fonctionnalités dans Excel qu'un ancien système d'exploitation ne supporte pas, comme une mise à niveau 5G pour Internet des objets, vous auriez besoin d'un Hard Fork. Un Hard Fork introduit des changements qui ne sont pas rétrocompatibles et nécessite une mise à jour du système pour implémenter ces fonctionnalités.

Cela est similaire au Hard Fork effectué sur la Blockchain Ethereum pour contourner les règles et propriétés rigides de la blockchain originale.

Soft Fork

- Changements mineurs du système
- Rétrocompatible
- Les nœuds n'ont pas besoin de se mettre à jour pour former un consensus

Hard Fork

- Changements majeurs du logiciel
- Non rétrocompatible
- Les nœuds doivent suivre les nouvelles règles de consensus

Leçons

- Tous les contrats ne sont pas intelligents ; leur efficacité dépend de leur mise en œuvre.
- Une fois déployé, un contrat ne peut pas être facilement corrigé.
- Si défectueux, un contrat peut compromettre l'immuabilité de la blockchain.

---

§ Blockchains Privées

La blockchain existe sous deux formes, et le cas d'utilisation est crucial :

- **Public** : Nous ne faisons pas confiance aux nœuds, donc nous avons besoin d'un groupe public pour valider les opérations pour la sécurité.
- **Privé** : Nous pouvons limiter la blockchain à des secteurs spécifiques pour optimiser certains domaines.

Cas d'utilisation Spécial

Utiliser les propriétés de la blockchain pour solidifier les données de manière sécurisée, par exemple dans les contrats bancaires entre parties. Avec le chiffrement des contrats sur un système blockchain, l'accès aux données est accordé uniquement aux parties intéressées et aux régulateurs. Cela assure un système sécurisé, efficace, immuable et incontestable. De plus, les protocoles d'application de contrats intelligents peuvent rationaliser et perturber la paperasse administrative, entraînant des économies de coûts significatives.

---

§ Les Propriétés de la Vision Blockchain

- **Transactions sécurisées, efficaces, immuables et incontestables**
  - Les transactions sont sécurisées, efficaces et ne peuvent être modifiées ou contestées une fois confirmées.
- **Suppression de nombreux intermédiaires**
  - La technologie blockchain réduit ou élimine la nécessité d'intermédiaires.
- **Un monde de coûts de transaction quasi nuls crée de nouveaux actifs**
  - Des coûts de transaction extrêmement bas peuvent conduire à la création de nouveaux types d'actifs.
- **Confiance dans le réseau plutôt que dans la Banque Centrale**
  - La confiance est placée dans le réseau décentralisé plutôt que dans les banques centrales. Cependant, les banques centrales peuvent introduire leurs propres cryptomonnaies.
- **Tokenisation de presque tout actif**
  - Presque tout actif peut être tokenisé, facilitant le commerce et la gestion.

- **Inclusion financière pour les non-bancarisés**
  - La blockchain peut fournir des services financiers à ceux qui n'ont pas accès à la banque traditionnelle.

Risques des Cryptomonnaies

- **La technologie est compliquée à comprendre**
  - La complexité de la technologie des cryptomonnaies peut être un obstacle à l'adoption généralisée et à la compréhension.
- **Le Far West des ICOs et des investisseurs suiveurs**
  - Les Offres Initiales de Coins (ICOs) peuvent être risquées en raison du manque de réglementation, entraînant des escroqueries potentielles et des investissements mal informés.
- **Volatilité extrême**
  - Les cryptomonnaies sont connues pour leur volatilité élevée des prix, ce qui peut entraîner des risques financiers significatifs.
- **Risque réglementaire**
  - L'environnement légal et réglementaire des cryptomonnaies est incertain et peut évoluer rapidement, impactant leur valeur et leur utilité.
- **Le débat sur la vie privée**
  - Il y a un débat et une préoccupation continus concernant les problèmes de confidentialité liés à l'utilisation des cryptomonnaies, y compris l'équilibre entre transparence et anonymat.

Suivi suggéré

Blockchain CheatSheet - Cryptographie & Signatures

Auteur : Kenneth Boldrini

4o mini