Blockchain

Blockchain presentation for developers

Petit Rappel sur la cryptographie

Les fonctions de hachage

Une fonction de hachage cryptographique est une fonction pure et déterministe qui prend en entrée un message de taille arbitraire et qui produit en sortie un ensemble de taille fixe. Ces sorties sont generalement appelées hash ou digest de l'entrée (input).

- **Determinisme** - Pour une entrée donnée, la sortie est toujours la même.
- **Vitesse** - En général quelques millisecondes pour calculer le hash d'un message.
- **Resistance aux collisions** - Il devrait etre difficile de trouver deux messages différents qui produisent le même hash.
- **non inversible** - Une fonction de hachage ne doit pas pouvoir être inversée pour retrouver le message d'origine à partir du hash.

Les fonctions de hashage sont au coeur du maintien de l'intégrité des base de données de type blockchain. Elles forment aussi la base du mécanisme de preuve de travail (Proof of Work) qui est utilisé pour sécuriser les blockchains de type Bitcoin.

Petit Rappel sur la cryptographie

La cryptographie asymétrique ou à clé publique

La cryptographie asymétrique est un type de cryptographie qui utilise une paire de clés pour le chiffrement et le déchiffrement. Une clé est publique et l'autre est privée. La clé publique peut être partagée avec tout le monde, tandis que la clé privée doit être gardée secrète.

Une chaine de caractères encrypée avec une clé publique ne peut être déchiffrée qu'avec la clé privée correspondante. Cela permet de créer des signatures numériques qui peuvent être vérifiées par n'importe qui ayant accès à la clé publique. Si on souhaite envoyer une message cryptés a une personne, on peut utiliser sa clé publique pour chiffrer le message. La personne pourra ensuite utiliser sa clé privée pour déchiffrer le message.

Petit Rappel sur la cryptographie

La cryptographie asymétrique ou à clé publique

Ces paires peuvent aussi être utilisées pour créer des signatures numériques.

Une signature numérique est un hash du message chiffré avec la clé privée. Cette signature peut être vérifiée par n'importe qui ayant accès à la clé publique. C'est le mecanisme d'authentification utilisé dans les blockchains de type Bitcoin (ou blockchains publiques). Beaucoup d'algorithme de cryptographie asymétrique existent, les plus connus sont RSA et ECDSA. Ethereum utilise ECDSA.

Armés de ces deux grands principes vous êtes maintenant prêts à comprendre le fonctionnement de la blockchain.

La blockchain en bref

Definition

"La blockchain est un registre numérique publique indélébile et décentralisé."

Une blockchain est une base de données **distribuée** et sécurisée. Elle est partagée par tous les **noeuds** du réseau et contient l'historique de toutes les **transactions** qui ont eu lieu depuis sa création. Chaque noeud du réseau possède une copie de la blockchain. Lorsqu'une transaction est enregistrée au sein de la blockchain, elle ne peut être modifiée. Il n'existe pas d'autorité unique de controle sur la base de données. Cette dernière est repliquée sur tous les noeuds d'un réseau peer-to-peer. Ce qu'on peut stocker dans une blockchain est limité par la taille des blocs et la taille des transactions, en revanche on peut stocker n'importe quel type de données(monnaies, code executable, medias...).

La blockchain en bref

Les transactions et les blocs

Au sein d'une blockchain, tout changement d'état fait partie d'une transaction.

Penser à une transaction comme une opération d'écriture atomique d'un utilisateur dans une base de données globale qui peut modifier un ou plusieurs enregistrements. N'importe quel utilisateur du réseau peut soumettre une transaction à exécuter. La façon dont les transactions sont traitées fait partie des règles de transition d'état de la blockchain. Une blockchain passe d'un état à un autre en traitant chaque transaction qu'elle reçoit. Par exemple, une blockchain qui gère une monnaie peut traiter les transactions comme des transferts de sa monnaie entre deux comptes : elle réduit le solde de l'expéditeur et augmente celui du destinataire du même montant. D'autres blockchains permettent même aux transactions de créer et d'exécuter des programmes complets sur la chaîne. Quand un utilisateur envoie une transaction il doit la signer cryptographiquement avec sa clé privée. De cette façon, la blockchain peut faire respecter le fait qu'un utilisateur spécifique peut déplacer un certain actif ou modifier un certain enregistrement. Cela introduit une notion de propriété par le détenteur d'une clé.

La blockchain en bref

Les transactions et les blocs

Les transactions sont groupées en blocs. Un bloc est un ensemble de transactions qui sont traitées ensemble.

Les blocs sont ensuite enchainés les uns aux autres pour former la blockchain. Les blocs constituent l'historique de la blockchain, chacun d'eux contient un ensemble de transactions qui changent son état. La façon dont les transactions sont choisies et ordonnées dans chaque bloc dépend des règles de consensus de la blockchain, que nous verrons dans quelques pages. Quand un bloc est ajouté à la blockchain, il est propagé à travers le réseau peer-to-peer à tous les noeuds. Chaque noeud va ré-exécuter toutes les transactions du bloc localement afin de vérifier si elles sont bien valides, rejetant le bloc s'ils remarquent un changement illégal. Cela signifie que chaque transaction est en fait exécutée une fois par chaque noeud du réseau entier. Cela permet à la blockchain d'être complètement décentralisée, puisque chaque noeud vérifie toutes les transactions qui sont exécutées. Cependant, cela a un coût : les frais de calcul imposent une limite au nombre de transactions qui peuvent être traitées par seconde par le réseau. En d'autres termes, la performance est échangée contre la décentralisation.

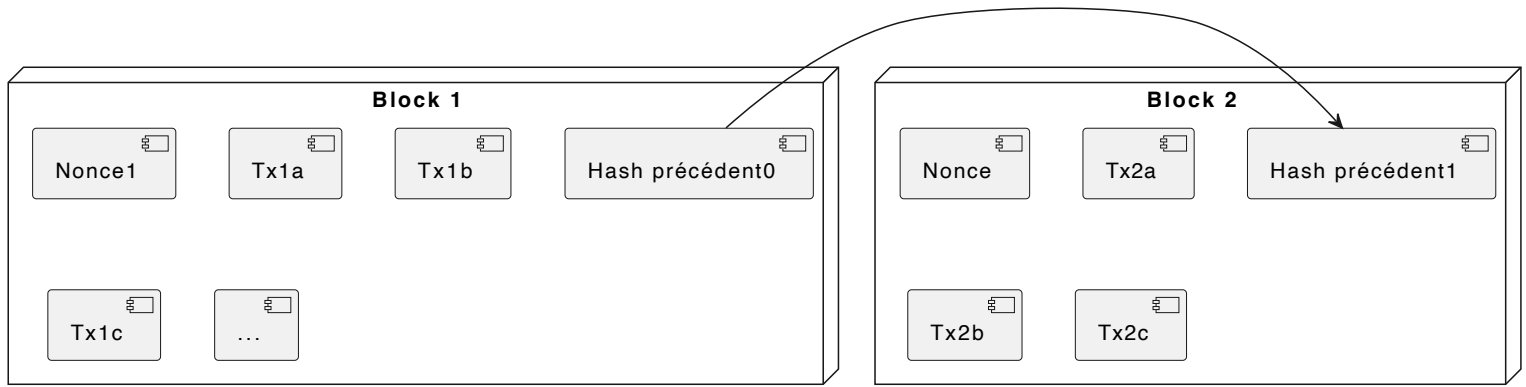
La blockchain en bref

Les transactions et les blocs

Le processus de validation des transactions et de création de nouveaux blocs est appelé **minage**.

Le coup de gestion des changements au sein d'une blockchain étant élevé, toutes les transactions nécessitent le paiement d'une taxe. Cette taxe est généralement payée dans une monnaie native à la blockchain (comme le bitcoin dans le réseau Bitcoin1 ou l'ether dans Ethereum). Quel que soit le bénéficiaire de cette taxe, que nous verrons dans quelques pages, l'objectif de la taxe est d'empêcher les attaquants de submerger le réseau avec des transactions qui doivent être traitées par chaque noeud, et de fournir une incitation aux noeuds qui ajoutent de nouveaux blocs à la chaîne.

La blockchain en bref
Une chaine de hash



Une blockchain est une chaine de hash. Chaque bloc contient un hash du bloc précédent. Cela permet de lier les blocs entre eux et de former une chaine. Si un bloc est modifié, son hash change et donc le hash du bloc suivant change aussi. Cela permet de détecter facilement les modifications sur la blockchain.

La blockchain en bref

Methodes de consensus

La blockchain est un système décentralisé. Il n'y a pas d'autorité centrale qui valide les transactions. Les noeuds du réseau doivent donc se mettre d'accord sur l'état de la blockchain. C'est le rôle des algorithmes de consensus.

Par exemple si un vendeur propose un bien sur la blockchain et que deux acheteurs se précipitent pour l'acheter, comment le réseau peut-il décider qui a acheté en premier ? Pire encore, comment empêcher le vendeur de dire aux deux acheteurs qu'ils ont fait l'achat et d'encaisser deux fois ? Nous devons trouver un moyen de déterminer comment les transactions sont choisies et ordonnées afin d'avoir un seul état de la blockchain. En d'autres termes, nous devons trouver un moyen d'établir un consensus sur les blocs qui sont ajoutés à la chaîne.

La blockchain en bref

Methodes de consensus

Beaucoup de blockchains publiques comme Bitcoin ou Ethereum utilisent (ou utilisaient) un algorithme de consensus connu sous le nom de **preuve de travail** (proof of work). Une preuve de travail est une preuve cryptographique qu'une quantité importante de ressource CPU a été dépensée pour effectuer un calcul; dans ce cas, calculer un nombre difficile basé sur un bloc. Pour qu'un bloc soit ajouté à la blockchain, il doit être accompagné de sa preuve de travail. N'importe quel noeud peut proposer un nouveau bloc et, s'il le soumet avec sa preuve de travail, il est ajouté à la blockchain. Le noeud qui peut ajouter un bloc reçoit une récompense en retour de son effort. Les noeuds qui remplissent ce rôle dans le réseau sont appelés mineurs, et chaque fois qu'un nouveau bloc est ajouté, ils se précipitent tous pour essayer d'ajouter le suivant pour capturer la récompense correspondante.

La blockchain en bref

Methodes de consensus

Le processus de minage est en fait un processus de résolution de puzzle.

Ce mecanisme est en réalité assez simple. L'identifiant de chaque bloc dans la chaine est un hash qui inclut l'identifiant du bloc précédent, toutes les transactions du bloc et un **nonce**. En changeant le nonce, le hash calculé sera complètement différent. Pour ajouter un nouveau bloc à la chaine, cet identifiant doit avoir une certaine structure (commencer par n zéros). Comme il n'est pas possible de prédire à quoi ressemblera un hash, un mineur ne peut que tenter de calculer le hash du bloc à plusieurs reprises en changeant le nonce jusqu'à ce qu'il obtienne un hash qui corresponde aux exigences. Cela nécessite de nombreuses tentatives et est donc considéré comme une preuve de travail.

Bitcoin

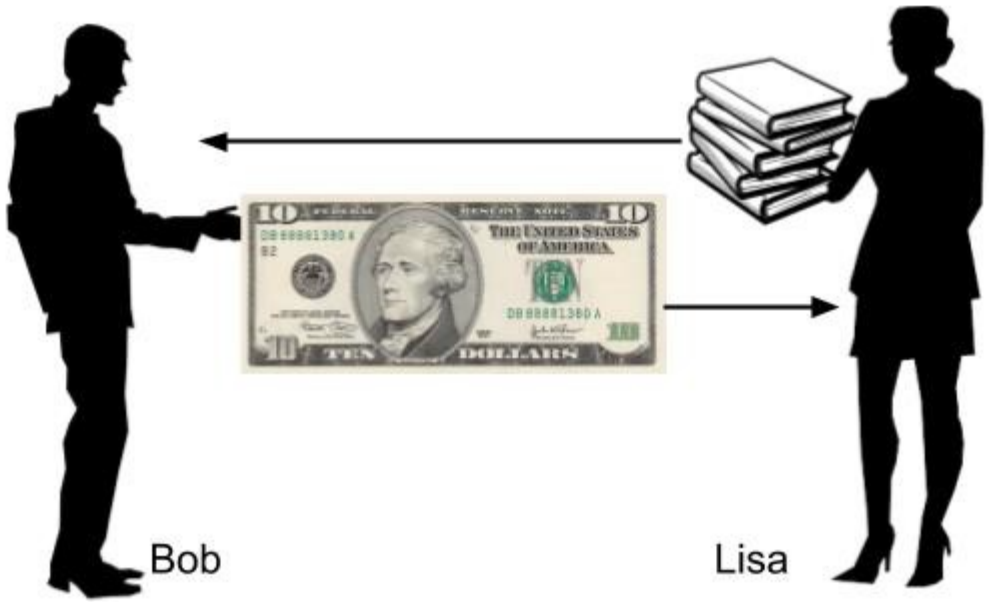
Présentation

Jusqu'ici nous avons décrit la blockchain en tant que base de données publique, mais nous n'avons pas encore parlé de ce que nous pouvons y stocker. Parlons maintenant de la première blockchain devenue célèbre pour traquer les transactions de sa monnaie numérique : Bitcoin.

Bitcoin

Double dépense (double-spending)

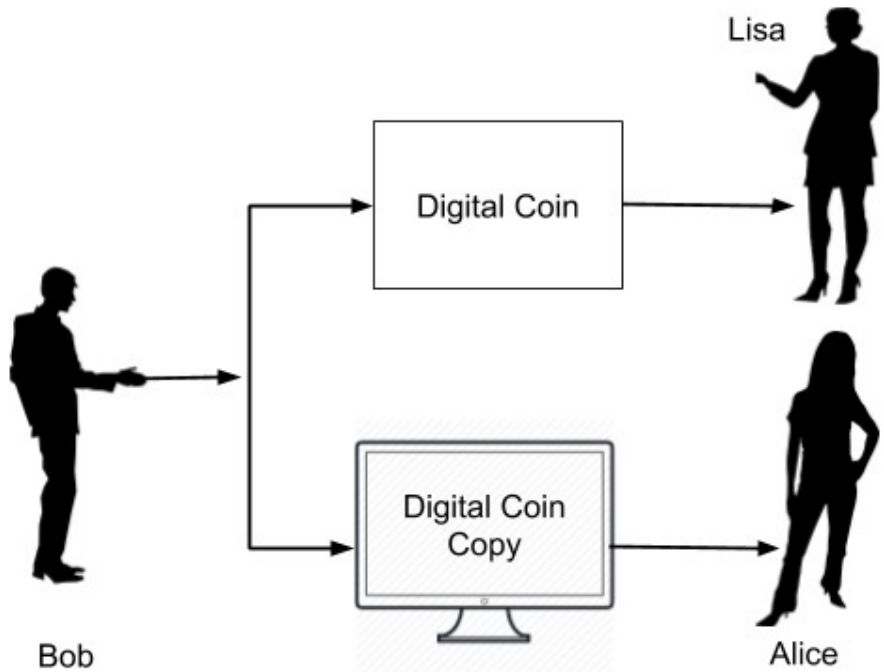
La blockchain Bitcoin vient résoudre le problème de la double dépense dans les systèmes de paiement électronique.



Bitcoin

Double dépense (double-spending)

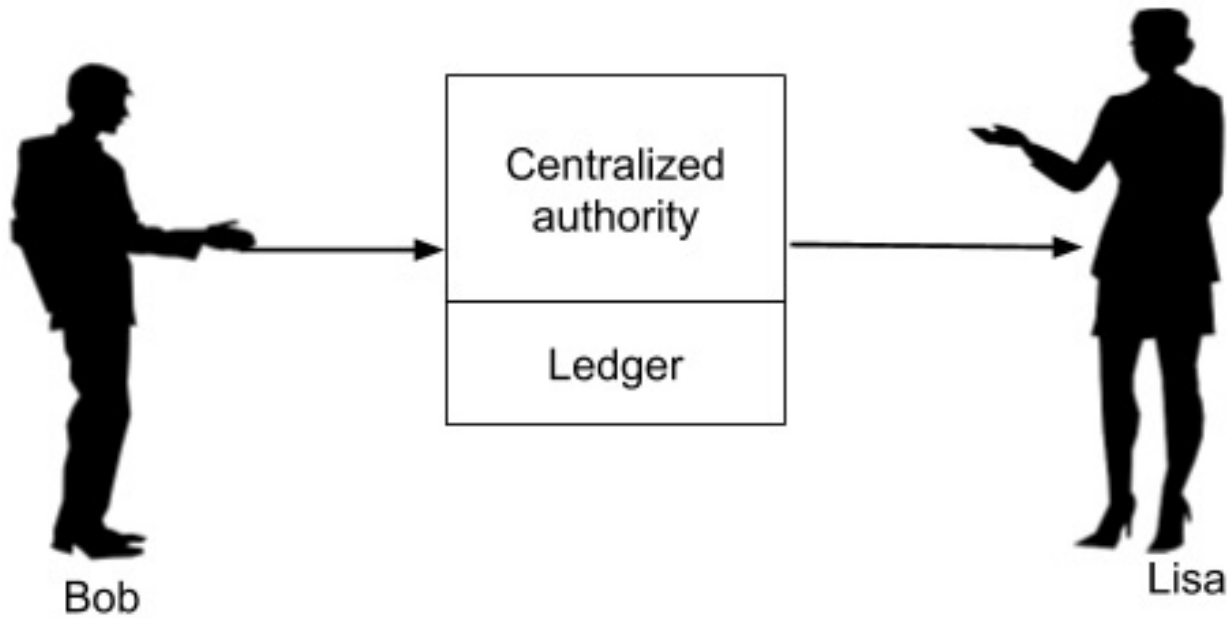
La blockchain Bitcoin vient résoudre le problème de la double dépense dans les systèmes de paiement électronique.



Bitcoin

Double dépense (double-spending)

La blockchain Bitcoin vient résoudre le problème de la double dépense dans les systèmes de paiement électronique.



Bitcoin

BTC (Bitcoin)

La plupart des grands principes des blockchains ont été présentés en 2008 par Satoshi Nakamoto dans son article "Bitcoin: A Peer-to-Peer Electronic Cash System". L'article est court et facile à lire, et il contient la plupart des concepts de blockchain utilisés aujourd'hui. Il présente une "version purement peer-to-peer de l'argent électronique", sans propriétaire ou émetteur centralisé.

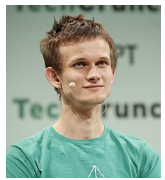
La blockchain Bitcoin est une base de données publique décentralisée qui garde une trace du solde en bitcoin de ses utilisateurs et prend en charge les transactions pour déplacer des fonds d'une adresse à une autre. C'est une implémentation d'une plateforme de paiement électronique décentralisée.

Il est important de mentinner que Bitcoin, en plus des transferts simples, prend également en charge un langage de script limité. Ce langage permet des constructions telles que les verrous temporels, qui restreignent l'exécution d'un transfert jusqu'à un certain moment dans le futur, ou les transactions multi-signatures, qui nécessitent que plusieurs comptes soient d'accord pour déplacer un actif. Cependant, ce qui peut être construit avec ce langage est encore limité.

Bitcoin paper

Ethereum
Smart contracts

La blockchain Ethereum est une blockchain publique décentralisée qui prend en charge les contrats intelligents (smart contracts).



Elle est présentée en 2013 par Vitalik Buterin et lancée en 2015. Sa principale particularité est la possibilité d'y déployer du code qui pourra être exécuté dans la blockchain sous forme de smart contracts.

Un smart contract est un court programme téléchargé dans la blockchain, qui peut réagir aux transactions qui lui sont envoyées en exécutant une logique arbitraire. Chaque smart contract a également son propre état arbitraire, qui peut être mis à jour sur n'importe quelle transaction et peut contenir n'importe quelle donnée. Et bien sûr, un smart contract peut également contenir de l'ETH, la monnaie native du réseau Ethereum.

Ethereum
Smart contracts

La blockchain Ethereum est une blockchain publique décentralisée qui prend en charge les contrats intelligents (smart contracts).

Le reseau Ethereum detient à la fois une monnaie numérique (l'ether) et du code executable (les smart contracts) avec leur propre état.

Cette flexibilité permet à Ethereum d'implémenter de nombreuses constructions différentes. Par exemple, une toute nouvelle monnaie peut être facilement implémentée sous la forme d'un smart contract. Le contrat n'a besoin que de garder une trace du solde de chaque utilisateur, et de fournir des méthodes pour les transférer en toute sécurité. Cela permet de créer de nouvelles crypto-monnaies sur Ethereum avec peu d'efforts.

Neanmoins, rappelez-vous que toutes les transactions sont ré-exécutées par tous les noeuds du réseau afin d'être vérifiées. Cela signifie que, bien que les smart contracts puissent exécuter un code arbitraire, ce code doit être déterministe. Il doit toujours donner le même résultat, peu importe quand ou où il est exécuté. Il ne peut pas non plus dépendre de sources externes à la blockchain; sinon, la validité de la blockchain devient dépendante de ces sources externes. Un

Ethereum
Les frais de Gaz (Gas fees).

Permettre à n'importe quel utlisateur d'envoyer une transaction avec du code arbitraire qui sera exécuté sur chaque noeud du réseau est potentiellement dangereux. Un utilisateur malveillant pourrait soumettre un code extrêmement coûteux à exécuter ou un code qui ne se termine jamais.

Pour se protéger contre cela, Ethereum introduit un concept appelé gaz. Pensez au gaz comme à la mesure de la puissance de calcul nécessaire pour traiter une transaction. Dans une transaction, les opérations complexes consommeront plus de gaz que les opérations plus simples. Par exemple, modifier le stockage du contrat est beaucoup plus coûteux qu'une simple expression arithmétique.

Une transaction envoyée au réseau nécessite une allocation de gaz pour être envoyée. Ce gaz est payé en ETH. Chaque ligne de code exécutée par la transaction consomme un peu de son gaz, et si elle tombe à zéro, le traitement est immédiatement arrêté et la transaction échoue. Néanmoins, son expéditeur est toujours facturé pour les tracas de traitement d'un processus aussi long.

L'expéditeur d'une transaction peut également définir le prix du gaz, indiquant qu'il est prêt à payer plus (ou moins) que les autres utilisateurs pour l'exécution de sa transaction. C'est un moyen de faire en sorte que leur transaction soit incluse dans la blockchain plus rapidement (ou moins cher) que les autres utilisateurs, en la rendant plus (ou moins) attrayante pour les mineurs.

Ethereum
Les applications décentralisées (DApps)

Les contrats intelligents permettent la construction d'applications décentralisées (DApps). Les DApps sont des applications web client-side qui ne sont pas hébergées sur un serveur, mais sur un ensemble de contrats intelligents sur la blockchain. Au lieu d'envoyer des requêtes HTTP à un serveur web, les utilisateurs de l'application envoient des transactions à un contrat intelligent sur le réseau Ethereum. Il est même possible d'héberger l'application web elle-même sur un système de stockage de fichiers décentralisé, ce qui rend l'application complètement indépendante de toute infrastructure centralisée.

Au lieu de consulter des données à partir d'un magasin de données centralisé, les applications décentralisées utilisent la blockchain comme source de vérité. Les données utilisées pour peupler l'application sont soit stockées sur la blockchain, soit sur un emplacement de stockage distant auquel on fait référence à partir de la blockchain. De même, la logique métier de l'application est codée dans un ensemble de contrats intelligents. Les utilisateurs effectuent des actions persistantes sur l'application en envoyant des transactions à ses contrats intelligents.

Ethereum
Les applications décentralisées (DApps)

Les contrats intelligents permettent la construction d'applications décentralisées (DApps). Les DApps sont des applications web client-side qui ne sont pas hébergées sur un serveur, mais sur un ensemble de contrats intelligents sur la blockchain. Au lieu d'envoyer des requêtes HTTP à un serveur web, les utilisateurs de l'application envoient des transactions à un contrat intelligent sur le réseau Ethereum. Il est même possible d'héberger l'application web elle-même sur un système de stockage de fichiers décentralisé, ce qui rend l'application complètement indépendante de toute infrastructure centralisée.

Au lieu de consulter des données à partir d'un magasin de données centralisé, les applications décentralisées utilisent la blockchain comme source de vérité. Les données utilisées pour peupler l'application sont soit stockées sur la blockchain, soit sur un emplacement de stockage distant auquel on fait référence à partir de la blockchain. De même, la logique métier de l'application est codée dans un ensemble de contrats intelligents. Les utilisateurs effectuent des actions persistantes sur l'application en envoyant des transactions à ses contrats intelligents.

Ethereum

Les applications décentralisées : experience utilisateur

Comment une DApp se présente-t-elle à un utilisateur ? Certaines DApps privilégieront la décentralisation à la facilité d'utilisation et demanderont aux utilisateurs d'y accéder avec un navigateur spécialisé ou une extension de navigateur. Ces extensions agissent comme des portefeuilles, détenant les clés de l'utilisateur, et comme une passerelle vers la blockchain en fournissant une connexion à un nœud Ethereum. Sous le capot, ils injectent un objet javascript qui fournit des méthodes de bas niveau pour accéder aux données de la blockchain et envoyer des transactions au nom de l'utilisateur. Chaque fois que l'application demande l'envoi d'une transaction, l'utilisateur se voit présenter une fenêtre contextuelle pour l'approuver. Cela déplace une grande partie de la complexité de la DApp vers l'extension, mais nécessite également un effort important de la part de l'utilisateur pour se mettre en place, en installant l'extension, en créant et en sauvegardant un compte, et en achetant de l'ETH pour commencer à fonctionner. Nous utiliserons cette approche pour construire notre première DApp et y reviendrons plus en détail lorsque nous verrons les détails de l'envoi de transactions.

Ethereum
Les applications décentralisées : experience utilisateur

D'autres DApps ont une approche plus conviviale pour l'utilisateur, gérant les clés au nom de l'utilisateur. Il est même possible pour un utilisateur d'utiliser une DApp sans même s'en rendre compte, si toute sa complexité est gérée en arrière-plan. Cependant, cela signifie également que l'utilisateur n'est plus maître de ses propres clés, mais délègue cette tâche à l'application. De plus, si chaque application gère son propre ensemble de clés, l'interopérabilité est beaucoup plus difficile, car l'utilisateur aura une identité différente sur chaque service. Nous explorerons les approches conviviales pour l'utilisateur, ainsi que les défis qu'elles posent. Dans l'ensemble, les bonnes applications offrent des expériences différentes à différents utilisateurs, en fonction de leur familiarité avec Ethereum.

Quelle que soit la gestion des clés, toutes les DApps doivent tenir compte des longs temps de confirmation du réseau. Dans les applications Web traditionnelles, une action sous la forme d'une requête HTTP prend quelques millisecondes pour arriver au serveur Web et revenir. Cependant, dans Ethereum, une transaction peut prendre plusieurs secondes pour être extraite,

Ethereum

Les applications décentralisées : pourquoi la blockchain ?

La première question que vous devriez vous poser lorsque vous implémentez un système basé sur la blockchain est de savoir si vous avez vraiment besoin d'une blockchain.

Il est facile de se laisser emporter par les cycles de hype en technologie : vous pouvez utiliser un cluster Kubernetes pour mettre à l'échelle horizontalement la charge sur votre application web qui fonctionnerait parfaitement sur une seule machine, ou vous pouvez utiliser des algorithmes d'apprentissage automatique de pointe pour déduire des tendances de votre ensemble de données avec moins de 100 entrées qui seraient mieux visualisées dans une feuille de calcul Excel. Des millions ont été dépensés dans le développement d'applications mobiles natives pour présenter des informations statiques, car c'était plus cool qu'un simple site web réactif.

La blockchain ne fait pas exception à la hype, avec le facteur aggravant qu'elle peut être utilisée comme instrument pour les spéculateurs financiers. N'oubliez jamais que, simplement parce que vous avez un nouveau marteau brillant entre les mains, tout ne devient pas un clou. Vous ne devriez pas essayer de

Ethereum

Les applications décentralisées : avantages

La finance décentralisée est l'un des cas d'utilisation les plus populaires.14 La première blockchain, Bitcoin, a été construite comme une plate-forme de paiement décentralisée, mais les applications financières d'une blockchain peuvent aller beaucoup plus loin. Les contrats intelligents peuvent être utilisés pour prendre en charge de nombreux types de flux de travail financiers, tels que les échanges décentralisés, les dérivés, le trading sur marge, les assurances, les crédits, les prêts, les investissements, les marchés de prédiction, etc. Ces artefacts nécessitaient traditionnellement que les utilisateurs placent leur confiance et leurs actifs dans une institution centralisée - cela augmentait la barrière à l'entrée, et l'institution prenait souvent une lourde commission pour ses services. Maintenant, un contrat intelligent dans une blockchain publique auditable peut agir comme l'institution soutenant ces services financiers, agissant sur les crypto-monnaies à l'intérieur de la chaîne.

En général, les blockchains brillent dans les scénarios où il y avait besoin d'un tiers de confiance, car elles agissent comme une plate-forme neutre crédible pour que plusieurs participants interagissent en toute sécurité. Cela ne s'applique pas seulement aux applications financières, mais aussi chaque fois qu'il y a besoin de vérifier publiquement la transparence d'un processus. Par exemple, dans une vente aux enchères en ligne, il est possible de vérifier que les offres de tous les participants sont traitées en les soumettant (chiffrées) à la

Ethereum

Les applications décentralisées : avantages

En enlevant le besoin d'un tiers de confiance, les contrats intelligents peuvent être utilisés pour créer des plateformes ou des protocoles sans confiance. Au lieu de construire sur une couche propriétaire, où les règles du jeu peuvent être modifiées unilatéralement par le propriétaire, vous pouvez construire sur une plate-forme décentralisée. Un bon exemple est un marché : les grandes entreprises traditionnelles qui exploitent des places de marché d'applications et de services peuvent modifier leurs conditions générales (et leur part !) à tout moment. D'autre part, un marché coordonné par un contrat intelligent est immuable et n'est géré par personne d'autre que la blockchain elle-même.

Un autre avantage d'une blockchain est celui de la permanence. Si vous, en tant qu'utilisateur, détenez quelque chose de valeur sur un système numérique et que le mainteneur d'un tel système disparaît, votre truc disparaît aussi. Cela peut être vrai non seulement pour les devises, mais aussi pour les actifs numériques, tels que les objets de collection ou les réalisations en ligne. Le fait d'avoir des actifs numériques enregistrés sur une blockchain garantit qu'ils sont maintenus indépendamment de l'organisation qui les a créés. Cela peut même permettre de négocier ces actifs au-delà des limites du système où ils ont été créés.