WATT NETWORK

Réseau de stockage décentralisé de la prochaine génération

(Version1.0.0)

Table des matières

Avant - propos

Au fur et à mesure que le monde devient de plus en plus numérique, le stockage décentralisé (IPFS) deviendra une tendance naturelle au développement de l'économie numérique.Watt sera le premier réseau de stockage décentralisé utilisé dans la vie quotidienne de tout le monde, marquant un grand pas en avant dans l'adoption du blockchain et du stockage distribué dans le monde entier.

Notre mission: mettre en place une plate - forme de contrat intelligente de stockage distribué que les gens ordinaires peuvent utiliser, qui est sûre et facile à utiliser.

Notre vision: créer le marché du stockage décentralisé le plus inclusif au monde, propulsé par Watt, le réseau de stockage décentralisé le plus largement utilisé au monde.

Introduction: pourquoi le stockage distribué est - il si important

Le monde est en train d'être numérisé. Depuis la naissance de la civilisation humaine, l'homme a inventé toutes sortes de technologies de stockage et de transmission de données, et la civilisation humaine a été transmise et conservée par les données.De l'oracle primitif à l'ordinateur de la civilisation moderne, la vitesse et la densité du partage des connaissances augmentent régulièrement avec les progrès de la technologie humaine.Les données sont produites, transférées, utilisées et stockées rapidement.En particulier, avec la maturité progressive de l'Internet des objets et la mise en place d'applications au cours des dernières années, la production et la transmission de données atteindront une échelle et une vitesse sans précédent.La société d'analyse des données, statista, a effectué des statistiques et des prévisions sur l'offre et la demande de stockage de données sur Internet et sur le trafic de données .D'un point de vue mondial,L'offre de stockage ne répond pas à la demande de stockage de données.En outre, les technologies de communication de cinquième génération (5G) seront bientôt disponibles dans le commerce, ce qui facilitera grandement la mise en place de l'IOT.Le coût du stockage et de la transmission des données sera un goulot d'étranglement qui limitera le développement de la technologie. La façon de stocker et de transmettre les données à moindre coût est devenue un problème urgent.Le stockage distribué basé sur blockchain nous fournit une nouvelle solution technique qui peut réduire considérablement le coût du stockage et de la transmission des données, tout en améliorant la sécurité du stockage des données.

I .Qu'est - ce que le stockage distribué basé sur blockchain?

Un système de stockage de données distribué est un réseau informatique dans lequel l'information est habituellement stockée sur plusieurs noeuds de façon répliquée.Il s'agit généralement d'une base de données distribuée où l'utilisateur stocke l'information sur plusieurs noeuds, ou d'un réseau informatique où l'utilisateur stocke l'information sur plusieurs noeuds du réseau Peer - to - peer.Le stockage distribué est

relatif au stockage centralisé.En bref, les données sont stockées sur plusieurs noeuds.La combinaison de blockchain et de stockage distribué est un système de stockage distribué basé sur blockchain.Le système peut être considéré comme une catégorie d'économie partagée.Les fournisseurs et les demandeurs de stockage et de trafic échangent des données et du trafic par l'intermédiaire de chaînes de blocs.Le réseau atteint progressivement l'équilibre entre l'offre et la demande sous l'équilibre de la chaîne de blocs.Les participants au système comprennent les fournisseurs de stockage et de trafic (qui connectent leurs propres dispositifs de stockage au système par l'intermédiaire du réseau et fournissent des services de stockage de données et de trafic) et les demandeurs de stockage et de trafic (qui paient pour l'accès au système).

II .Situation actuelle de l'industrie du stockage distribué blockchain

Les travaux de recherche et de développement sur les projets de stockage réparti basés sur blockchain ont débuté entre 2014 et 2015.À ce jour, il y a environ cinq ans.Le plus représentatif d'entre eux est le projet ipfs + filecoin en cours de développement.Le système se compose de deux Protocoles: le Protocole ipfs et le Protocole filecoin.Protocole ipfs: le nom complet est le système de fichiers interplanétaires, qui est défini comme suit:Un Protocole de transport hypermédia point à point, similaire au Protocole http.Protocole filecoin: projet de stockage distribué basé sur blockchain.

Tout d'abord, nous examinons les problèmes et l'orientation fonctionnelle des deux Protocoles.I p f s: distribution et localisation des données (Protocole de transfert de données, similaire au Protocole H T p).Transfert: les données sont transférées entre les noeuds.Localisation: adresse des données, emplacement de stockage des données trouvées.Filecoin: Data store (Like A cloud Store).Commerce de l'espace de stockage: stockage entre l'utilisateur et le mineur

Le commerce de l'espace, les mineurs "accrochent" leur propre espace de stockage au système à vendre, les utilisateurs achètent l'espace de stockage pour stocker leurs propres données.Transaction de bande passante: transaction de trafic de données entre les utilisateurs et les mineurs, les mineurs voient leurs propres données stockées vendues, les utilisateurs paient pour télécharger.Maintenance du réseau blockchain: les mineurs contribuent à la maintenance du réseau,Gain supplémentaire.Les transactions sur l'espace de stockage et la bande passante sont collectivement appelées marchés d'échange de valeur.Filecoin résout l'échange de valeur entre le stockage des données et le téléchargement des données par blockchain. Le nombre total de jetons fi le c oi n est de 2 milliards.Comme dans le système bitcoin, la distribution initiale des jetons se fait par l'intermédiaire de mineurs "Mining".Les jetons de filecoin sont émis linéairement.

L'un des défis liés à la tenue de transactions distribuées est la sécurité - plus précisément, la façon d'avoir un grand livre ouvert et modifiable tout en prévenant les activités frauduleuses.Pour relever ce défi, filecoin a introduit un nouveau processus appelé Mining (qui utilise l'algorithme consensuel « work Proof ») afin de déterminer qui est « fiable », mettant ainsi à jour le dossier partagé de la transaction.Vous pouvez considérer l'exploitation minière comme un jeu économique qui oblige les « validateurs

» à prouver leur valeur lorsqu'ils tentent d'ajouter une transaction à un dossier.Pour vérifier, le validateur doit résoudre une série de problèmes informatiques complexes.Les contributeurs qui résolvent d'abord ce problème recevront des récompenses pour permettre la publication des derniers blocs de négociation.La publication du dernier bloc de négociation permet au vérificateur de « creuser » un bloc de récompense.Ce processus est très sûr, mais il nécessite beaucoup de puissance de calcul et de consommation d'énergie, parce que les utilisateurs « brûlent de l'argent » pour résoudre les problèmes de calcul et gagner plus de filecoin.C'est tellement punitif de brûler de l'argent contre des récompenses,De sorte qu'il est toujours dans l'intérêt du vérificateur de publier des transactions honnêtes dans les dossiers de filecoin

III.Problème: le stockage distribué n'atteint pas le public et un grand nombre d'utilisateurs n'utilisent pas leur espace de stockage inutilisé.

Dans les premiers jours de filecoin, il n'y avait que quelques personnes qui validaient les transactions et creusaient le premier bloc, et n'importe qui pouvait gagner de l'argent en exécutant le logiciel d'extraction de filecoin sur un PC.Au fur et à mesure que filecoin devient populaire, les mineurs intelligents se rendent compte qu'ils peuvent gagner plus s'ils ont plus d'un ordinateur à exploiter.

Au fur et à mesure que la valeur de filecoin continue d'augmenter, un grand nombre d'entreprises commencent à se préparer à la construction d'une mine.Les entreprises ont mis au point des puces spécialisées (« asic») et les ont utilisées pour construire une vaste base de serveurs pour exploiter filecoin.L'émergence de ces grandes sociétés minières a alimenté la ruée vers l'or de filecoin, ce qui rend difficile pour les gens ordinaires de contribuer au réseau et d'obtenir des rendements.Leurs efforts ont également commencé à consommer de plus en plus d'énergie informatique, ce qui a entraîné des problèmes environnementaux mondiaux croissants.

La commodité de l'exploitation minière de filecoin et l'essor subséquent des mines de filecoin ont rapidement contribué à la concentration à grande échelle de la productivité et de la richesse du réseau de filecoin.Pour fournir des renseignements généraux, 87% des filecoins sont maintenant détenus par 1% du réseau filecoin, dont beaucoup ont été extraits presque gratuitement au début.Un autre exemple est bitmain, l'une des plus grandes entreprises minières de filecoin,Des milliards de dollars de revenus et de profits ont été réalisés.

La concentration du pouvoir dans le réseau filecoin est très difficile et coûteuse pour les gens ordinaires.Si vous souhaitez obtenir filecoin, vos choix les plus simples sont:

1. Creusez vous - même.Il suffit d'avoir du matériel spécialisé (si vous êtes intéressé, voici une plateforme sur Amazon!)Alors va te changer.Sachez juste que, puisque vous serez en concurrence avec de grandes fermes de serveurs du monde entier, vous consommerez autant d'énergie que l'ensemble du pays Suisse, et vous ne pourrez pas exploiter trop de ressources.

2. Acheter filecoin à la bourse.Aujourd'hui, au moment de la rédaction de cet article, vous pouvez acheter filecoin pour 3500 $l'unit é (Remarque: Vous pouvez acheter une partie du nombre de filecoin!)Bien entendu, cela comporte également des risques importants en raison de l'instabilité des prix de filecoin.

Filecoin montre pour la première fois comment la crypto - monnaie peut briser le modèle financier actuel et permettre aux gens de faire des transactions sans entrave de tiers.L'augmentation de la liberté, de la flexibilité et de la protection de la vie privée continue de faire de la monnaie numérique une nouvelle norme inévitable.Malgré les nombreux avantages de filecoin,Mais la concentration de son financement et de son pouvoir (peut - être par inadvertance) constitue un obstacle important à l'application courante.L'équipe centrale de Watt a mené une étude pour comprendre pourquoi les gens ne veulent pas entrer dans le domaine de la cryptographie.Le risque d'investissement et d'exploitation minière a toujours été considéré comme un obstacle majeur à l'entrée sur le marché.

Filecoin est basé sur un disque dur de grande capacité pour l'exploitation minière, ce qui conduit à une centralisation et une monétisation excessives et ne peut pas atteindre le public. Avec le développement de la technologie mobile, l'équipement terminal de l'utilisateur a beaucoup d'espace libre et la capacité n'est pas utilisée. Il s'agit d'un marché de stockage distribué avec un grand espace. Watt est basé sur l'espace libre de l'extrémité mobile et fournit un stockage distribué innovant pour la téléphonie mobile.

IV.Solution: mise en œuvre de l'exploitation minière Watt et du stockage distribué sur les terminaux mobiles

Après avoir identifié les principaux obstacles à l'adoption, l'équipe centrale du Watt a commencé à chercher un moyen de permettre aux gens ordinaires d'exploiter (ou d'obtenir des récompenses en crypto - monnaie en validant les transactions pour les transactions distribuées).En tant que gardien, l'un des principaux défis de la tenue d'un dossier de transaction distribué est de s'assurer que la mise à jour de ce dossier public n'est pas frauduleuse.Bien que le processus de mise à jour des enregistrements de bitcoin ait été prouvé (brûler de l'énergie / de l'argent pour prouver la crédibilité), il n'est pas très bon utilisateur (ou planète!)Amical.En ce qui concerne Watt, nous avons introduit une exigence de conception supplémentaire, à savoir que le CPS utilise un algorithme de cohérence qui est très convivial pour les utilisateurs et qui, idéalement, peut être exploité sur des ordinateurs personnels et des téléphones mobiles.

En comparant les algorithmes de cohérence existants (processus d'enregistrement des transactions dans le grand livre distribué), le Protocole de cohérence Stellar est devenu le principal candidat pour soutenir l'exploitation minière préférentielle mobile conviviale.Le Protocole du consensus stellaire (SCP) a été conçu par David Mazi, professeur d'informatique à l'Université de Stanford et scientifique en chef à la star Development Foundation.SCP utilise un nouveau mécanisme appelé Federated Byzantine Agreement pour s'assurer que les mises à jour du grand livre distribué sont

exactes et fiables.SCP est également déployé dans la pratique par le biais de la chaîne Stellar blockchain, qui fonctionne depuis 2015.

V .Introduction au Protocole sur le consensus stellaire

Watt utilise d'autres types d'algorithmes de cohérence et est basé sur le Protocole sellar consensus (SCP) et un algorithme appelé Federated by zantin Agreement (FBA).Ces algorithmes ne gaspillent pas d'énergie, mais ils doivent échanger de nombreux messages réseau afin que les noeuds puissent « s'entendre » sur ce qu'est le prochain bloc.Chaque noeud peut déterminer indépendamment si une transaction est valide.Par exemple, l'autorisation de convertir et de répéter les frais généraux est déterminée en fonction de la signature chiffrée et de l'historique des transactions.Toutefois, pour qu'un réseau informatique puisse s'entendre sur les transactions à enregistrer dans un bloc et sur l'ordre de ces transactions et blocs, il faut qu'ils envoient des messages les uns aux autres et qu'ils votent à plusieurs tours pour parvenir à un consensus.Intuitivement,L'information des différents ordinateurs du réseau sur le bloc suivant ressemble à ceci: « Je suggère que nous votions tous pour que le bloc a soit le bloc suivant; »J'ai voté pour le bloc a comme prochain bloc ";"Je confirme que la plupart des noeuds en qui je fais confiance votent également pour le bloc A. À partir de cet algorithme de cohérence, le noeud peut conclure que « A est le bloc suivant;Aucun autre bloc que a n'est le bloc suivant ";Bien que les étapes de vote ci - dessus semblent nombreuses, Internet est assez rapide et l'information est légère, de sorte que cet algorithme de cohérence n'est pas seulement une preuve de travail.L'un des principaux représentants de cet algorithme est connu sous le nom d'algorithme général byzantin.Certaines des chaînes d'anneaux de blocs de haut niveau d'aujourd'hui sont basées sur des variantes bft telles que NEO et Ripple.

L'une des principales critiques du bft est qu'il a un point de concentration: parce qu'il s'agit d'un vote, l'ensemble des noeuds qui participent au vote "quorum" est déterminé au départ par l'ensemble des créateurs du système.La contribution de FBA est que chaque noeud a son propre "Groupe de quorum" au lieu d'un quorum déterminé centralement,Ces groupes de quorum forment à leur tour des quarts différents.Les nouveaux noeuds peuvent rejoindre le réseau de manière décentralisée: ils déclarent les noeuds en qui ils ont confiance et convainquent les autres noeuds de leur faire confiance, mais ils n'ont pas besoin de convaincre une autorité centrale.

SCP est un exemple de FBA.Contrairement à la consommation d'énergie de filecoin et à l'algorithme traditionnel de cohérence de la preuve de travail de la monnaie numérique, les noeuds SCP protègent les enregistrements partagés en s'assurant que les autres noeuds du réseau sont fiables.Chaque noeud du réseau construit un quorumslice, qui se compose d'autres noeuds du réseau qu'ils considèrent comme fiables.Les fourchettes sont établies sur la base du quorum de ses membres,Et le validateur n'acceptera une nouvelle transaction que si et seulement si une partie des noeuds de la portée acceptent également la transaction.Étant donné que les validateurs de l'ensemble du réseau construisent leurs lignes directrices, ces lignes directrices aident les noeuds à parvenir à un consensus sur les transactions tout en assurant la sécurité.Vous

pouvez en savoir plus sur le Protocole de cohérence stellaire en regardant cette courte vidéo d'explication de 7 minutes ou en regardant le résumé technique du SCP.

VI.Itération du Protocole de consensus stellaire (SCP) par watt

L'algorithme de cohérence Watt est basé sur SCP.SCP a été officiellement certifié [mazieres 2015] et est actuellement mis en œuvre dans le réseau stellaire.Contrairement au réseau Stellar, qui est principalement composé d'entreprises et d'institutions comme IBM, watt a l'intention de permettre aux appareils personnels de contribuer et de recevoir des récompenses au niveau du Protocole, y compris les téléphones mobiles, les ordinateurs portables et les ordinateurs.Voici comment Watt applique le SCP à l'exploitation minière personnelle.

Les utilisateurs peuvent jouer deux rôles, à savoir:

• mineurs.Les utilisateurs d'applications mobiles Watt confirment simplement chaque jour qu'ils ne sont pas des « robots ».Cet utilisateur vérifie son existence chaque fois qu'il se connecte à l'application.Ils peuvent également ouvrir l'application pour demander une transaction (par exemple, payer une autre société pionnière avec watt)

• noeuds.Un pionnier dans l'utilisation d'applications mobiles Watt, un contributeur et l'exécution du logiciel de noeud Watt sur leur bureau ou ordinateur portable.Watt Node Software est le logiciel qui exécute l'algorithme SCP de base. Ce logiciel se réfère aux informations de carte de confiance fournies par le contributeur.

Les utilisateurs peuvent jouer plusieurs de ces rôles.Tous les rôles sont nécessaires, de sorte que tous les rôles reçoivent de nouvelles pièces Watt sur une base quotidienne, à condition qu'ils participent et contribuent à ce jour.Dans la définition lâche du mineur, le mineur est l'utilisateur qui reçoit une nouvelle pièce comme récompense de contribution, et tous les rôles sont considérés comme des mineurs watt.Notre définition de l '« exploitation minière » est plus large que celle de l' « algorithme de cohérence de la preuve de l'exécution du travail », comme dans bitcoin ou Ethernet.

1.Node

Pour faciliter la lecture, nous définissons le noeud de connexion correct mentionné dans l'article SCP comme un noeud complet.De plus, pour des raisons de lisibilité, nous définissons le réseau Watt primaire comme une collection de tous les noeuds complets du réseau watt.La tâche principale de chaque noeud est configurée pour se connecter correctement au réseau Watt primaire.Intuitivement,Un noeud mal connecté au réseau primaire est similaire à un noeud blockchain qui n'est pas connecté au réseau bitcoin primaire.

2.Utilisateurs d'applications mobiles

Lorsque l'avant - garde doit confirmer qu'une transaction donnée a été effectuée (p. ex., qu'elle a été reçue)π),Ils ouvrent l'application mobile.À ce stade, l'application mobile se connecte à un ou plusieurs noeuds pour vérifier si la transaction a été

enregistrée dans le grand livre et pour obtenir le dernier numéro de bloc et la valeur de hachage du bloc.Si Pioneer avait aussi un noeud,L'application mobile se connectera alors à son propre noeud.Si Pioneer n'exécute pas un noeud, l'application se connecte à plusieurs noeuds et vérifie l'information.Les pionniers peuvent choisir les noeuds auxquels ils veulent que leurs applications se connectent.Mais pour que la plupart des utilisateurs soient simples, l'application devrait avoir un ensemble raisonnable de noeuds par défaut.Par exemple, certains des noeuds les plus proches de l'utilisateur sont basés sur des cartes de confiance et des noeuds choisis au hasard avec un pagerank élevé.Nous vous demandons de nous faire part de vos commentaires sur la façon de sélectionner l'ensemble de noeuds par défaut pour mobile Pioneer.

3.Prix de l'exploitation minière

Une caractéristique supérieure de l'algorithme SCP est qu'il est plus polyvalent que blockchain.Il coordonne la cohérence de l'ensemble du système de noeuds distribués.Cela signifie que le même algorithme de base est utilisé non seulement pour enregistrer de nouvelles transactions dans de nouveaux blocs toutes les quelques secondes, mais aussi pour exécuter périodiquement des calculs plus complexes.Par exemple,Le réseau stellaire l'utilise une fois par semaine pour calculer l'expansion du réseau stellaire et pour répartir les nouveaux jetons proportionnellement à tous les détenteurs de pièces stellaires (les pièces stellaires sont appelées lumens).De même, le réseau Watt utilise SCP une fois par jour pour calculer la distribution des nouvelles pièces Watt détenues par tous les mineurs watt (pionniers, contributeurs, ambassadeurs, noeuds).En d'autres termes, watt Currency Mining Rewards n'est calculé qu'une seule fois par jour.Pas dans chaque bloc.

Bitcoin attribue relativement des récompenses minières à chaque bloc et récompense tous les mineurs qui ont la chance de résoudre des tâches aléatoires intensives en calcul.À l'heure actuelle, un seul mineur reçoit 12 bitcoin (environ 60 000 $) toutes les 10 minutes.Cela rend très improbable qu'un mineur donné soit récompensé.Pour résoudre ce problème,Les mineurs de filecoin sont organisés dans des bassins d'excavation centralisés, ce qui permet d'améliorer la capacité de traitement, d'augmenter les chances d'obtenir des récompenses et, finalement, de les partager proportionnellement.Non seulement les bassins miniers sont - ils un élément central de la centralisation, mais leurs exploitants sont réduits, ce qui réduit les montants versés aux mineurs indépendants.Dans Watt, il n'est pas nécessaire d'exploiter les ressources.Parce que chaque contributeur reçoit une nouvelle allocation de jetons chaque jour.

4.Frais de transaction

Comme pour les transactions en bitcoin, la tarification sur le réseau Watt est facultative.Chaque bloc a une limite au nombre de transactions qu'il contient.Les transactions sont souvent libres lorsqu'il n'y a pas d'arriéré.Cependant, s'il y a plus de transactions, les noeuds sont triés par ordre de charge, les transactions les plus facturées sont en haut, et seules les transactions les plus élevées à inclure dans le bloc de construction sont sélectionnées.Cela en fait un marché ouvert.Méthode de mise en œuvre: répartir les dépenses entre les noeuds au pro rata une fois par jour.Dans chaque

bloc, le coût de chaque transaction est transféré dans un portefeuille temporaire qui, à la fin de la journée, est distribué aux mineurs actifs de la journée.Ce portefeuille a une clé privée inconnue.Avec l'accord unanime de tous les noeuds,L'accord lui - même impose des transactions à l'intérieur et à l'extérieur de ce portefeuille, tout comme il est convenu que de nouvelles pièces Watt sont frappées chaque jour.

VII. Brève introduction de l'algorithme de consensus de Watt mobile Distributed Storage

L'algorithme de consensus de Watt mobile Distributed Storage se compose de quatre nouveaux composants.

1. Réseau de stockage décentralisé

Réseau de stockage décentralisé (DSN): Watt fournit une abstraction d'un réseau de fournisseurs de services indépendants qui fournissent des services de stockage et de récupération.Ensuite, watt a proposé le Protocole Watt comme incitation, vérification et vérification de la construction du DSN.Les DSN regroupent le stockage fourni par plusieurs fournisseurs de stockage indépendants et peuvent fournir des services de stockage et de récupération de données aux clients de façon autonome.Cette coordination est décentralisée et n'a pas besoin de confiance: grâce à la coordination du Protocole, les participants individuels peuvent effectuer des opérations de vérification et le système peut obtenir des opérations de sécurité.Les DSN peuvent utiliser différentes stratégies de coordination, y compris le Protocole byzantin, le Protocole Gossip ou les crdts, selon les besoins du système.

2. Nouveau certificat de stockage

Watt propose deux nouveaux systèmes de preuve de stockage: la preuve de réplication permet au fournisseur de stockage de prouver que les données ont été répliquées à son seul périphérique de stockage physique dédié.L'exécution d'une copie physique unique permet au vérificateur de vérifier que le certificateur n'a pas copié plusieurs copies de données dans le même espace de stockage.

"Preuve de réplication" (porep)

Le Proof of Space Time permet aux fournisseurs de stockage de prouver que certaines données sont stockées dans la mémoire au moment spécifié.La preuve de réplication (porep) est un nouveau type de preuve de stockage.Il permet au serveur (certificateur p) de convaincre l'utilisateur (validateur v) que certaines données d ont été copiées sur son seul stockage physique dédié.Le schéma de Watt est un protocole interactif.Lorsque le certificateur P:S'engager à stocker n copies différentes (copies physiques indépendantes) d'une donnée d, puis (b) convaincre le vérificateur V, P par Protocole de réponse a effectivement stocké chaque copie.À la connaissance de Watt, porp a amélioré les solutions PDP et por, empêchant le piratage, l'externalisation et l'attaque par procuration.

Preuve spatio - temporelle (Post)

Le système de certification du stockage permet à l'utilisateur de demander la vérification que le fournisseur de stockage a stocké les données externalisées à ce moment - là.Comment Watt utilise - t - il le système pos pour démontrer que les données ont été stockées pendant un certain temps?Une réponse naturelle à cette question est de demander aux utilisateurs d'envoyer des demandes répétées (par exemple chaque minute) au fournisseur de stockage.Cependant, la complexité de la communication requise pour chaque interaction devient un goulot d'étranglement pour des systèmes comme Watt, car les fournisseurs de stockage sont tenus de soumettre leurs preuves aux réseaux blockchain.

Pour répondre à cette question, watt introduit une nouvelle preuve, la « preuve spatio - temporelle », qui permet au vérificateur de vérifier si le fournisseur de stockage a stocké ses données externalisées pendant un certain temps.Les exigences immédiates pour les fournisseurs sont les suivantes: (1) produire une preuve de stockage séquentielle (dans le cas du Watt, une « preuve de réplication ») comme méthode de détermination du temps.Former une exécution récursive pour générer une preuve simple.

3. Marché des Watt

Watt modélise les demandes de stockage et les exigences de récupération en tant que commandes pour deux marchés validables décentralisés exploités par le réseau watt.Le marché de la validation garantit qu'un paiement peut être effectué lorsqu'un service est correctement fourni.Watt décrit les marchés de stockage et de récupération où les clients et les mineurs peuvent soumettre des commandes de stockage et de récupération séparément.Watt a deux marchés:Marchés de stockage et de récupération.Les deux marchés ont la même structure mais des conceptions différentes.Le marché du stockage permet aux clients de payer pour le stockage de données par les mineurs.La récupération des données permet aux clients de payer les mineurs pour la livraison des données de récupération.Dans les deux cas, les clients et les mineurs peuvent fixer des prix cotés et des prix de demande ou accepter des prix courants.Cette transaction est gérée par le réseau - tous les noeuds du Watt sont anthropomorphes.Le réseau garantit que les mineurs sont récompensés par leurs clients pour leurs services.

Marché de la validation

Les marchés de négociation sont des accords qui facilitent l'échange de biens et de services spécifiques.Ils permettent aux acheteurs et aux acheteurs de faciliter les transactions.Pour le Watt, le watt exige que la transaction soit vérifiable: Les participants au réseau décentralisé doivent être en mesure de valider la transaction entre l'acheteur et le vendeur.Watt propose le concept de marché de validation.Il n'a pas d'entité unique pour gérer les transactions, qui sont transparentes,N'importe qui peut participer anonymement.Les accords de marché vérifiables permettent de décentraliser les transactions de services: la cohérence des carnets de commandes, le règlement des

commandes et l'exécution correcte des services peuvent être vérifiés indépendamment par les participants - mineurs et noeuds entiers dans le watt.

Marché du stockage

Le marché du stockage est un marché vérifiable qui permet aux clients (c. - à - d. Les acheteurs) de demander leurs données de stockage et aux mineurs de stockage (c. - à - d. Les vendeurs) de fournir leur espace de stockage.

Rechercher le marché

Le marché de la récupération permet aux clients de demander la récupération de données spécifiques, ce service étant fourni par le mineur de récupération.Contrairement aux mineurs de stockage, la récupération des mineurs n'exige pas de stockage de données ou de production de certificats de stockage pour une période donnée.N'importe quel utilisateur du réseau peut devenir un mineur de recherche et gagner un jeton Watt en fournissant un service de recherche.Récupération les mineurs peuvent soit recevoir des fragments de données directement du client, soit les récupérer, soit les stocker en tant que mineurs de stockage.

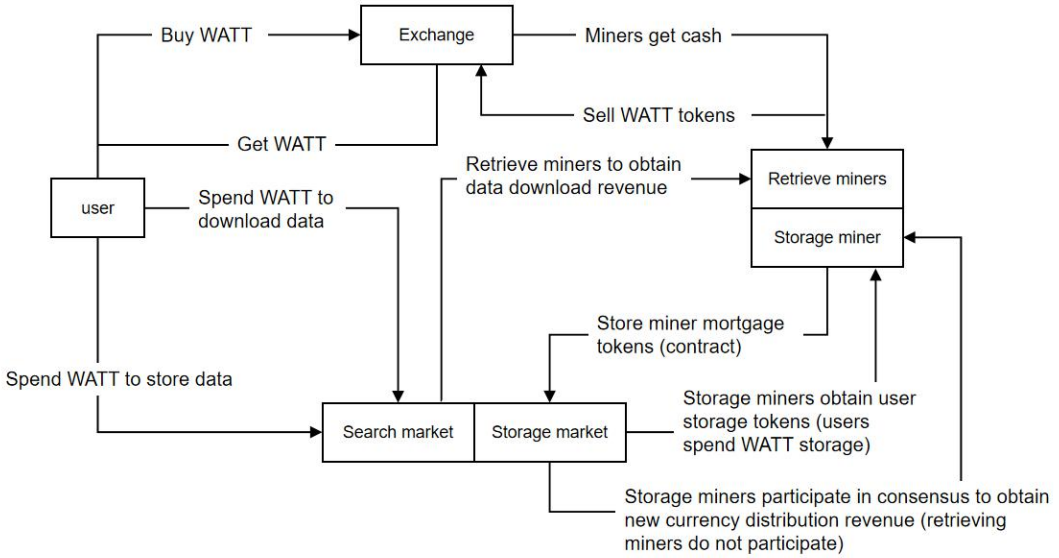
4. Preuve de la charge de travail effective (Proof - of - work)

Watt montre comment construire une preuve efficace de la charge de travail basée sur la « preuve spatio - temporelle » pour s'appliquer aux protocoles consensuels.Les mineurs n'ont pas besoin de calculs inutiles pour extraire le minerai, mais ils doivent plutôt stocker les données dans le réseau.Le Protocole Watt peut mettre en œuvre la démonstration Watt sur n'importe quel protocole consensuel qui permet la validation.Dans cette section,Comment le watt réglera - t - il les comptes en fonction de ce qui est disponible pour guider un accord consensuel?Les mineurs Watt produisent des « preuves spatio - temporelles » pour participer au consensus plutôt que de gaspiller des POW.Utile si la sortie calculée est précieuse pour le réseau, pas seulement pour assurer la sécurité de blockchain.

Ⅷ. Modèle économique Watt: un équilibre entre rareté et accessibilité

1.Principe de fonctionnement économique et écologique du Watt

Expliquons brièvement comment fonctionne le système watt (comme le montre la figure 1):



(1) Watt blockchain (Middle part): blockchain enregistre l'emplacement du stockage de données sur l'ensemble du réseau, ainsi que l'espace de stockage fourni par un mineur et les transactions sur l'ensemble du réseau.Blockchain paie les mineurs en fonction de leur contribution.

(2) Marché du stockage (ci - dessus): les utilisateurs soumettent leurs propres données, les mineurs acceptent les données des utilisateurs et les stockent dans leur propre espace de stockage, tout en recevant les frais payés par les utilisateurs.

(3) Récupérer le marché (partie suivante): l'utilisateur soumet ses propres

exigences de téléchargement de données, le mineur envoie les données à l'utilisateur après avoir reçu la commande, et obtient les frais payés par l'utilisateur.Ensemble, le blockchain Watt sert d'intermédiaire pour effectuer des transactions de valeur entre les utilisateurs et les mineurs.Les utilisateurs obtiennent des services de stockage de données et de trafic.Le mineur reçoit les frais de stockage et de débit payés par l'utilisateur.Entre - temps, les mineurs contribuent au fonctionnement normal du réseau de maintenance des ressources. Blockchain récompense les mineurs sous forme de monnaie numérique en fonction de leur contribution. C'est le problème résolu par ipfs + Watt + mobile.Regardons à nouveau la conception du système économique Watt et l'échange et le transfert de valeur: la conception du système économique est un élément important du projet blockchain.La robustesse de la conception du système économique détermine directement si le projet peut fonctionner à long terme.

Le système économique du Watt est conçu comme un modèle déflationniste, semblable à bitcoin: il a une certaine valeur de stockage.Le marché du stockage et le marché de la recherche polaire du Watt sont proches d'une économie de marché pleinement concurrentielle.Watt a son propre marché de valeur, et les jetons ont une forte valeur de circulation.Comme le montre la figure 1 ci - dessus, le modèle de génération et de circulation des jetons dans le système économique du Watt est comparé au watt.Watt est évidemment plus compliqué dans la circulation des jetons.En

récupérant et en stockant les jetons en circulation sur le marché, il s'agit également d'une représentation visuelle du marché de la valeur du Watt.

(1) Distribution des jetons initiaux: le nombre total de jetons Watt est de 20 milliards.Comme dans le système bitcoin, la distribution initiale des jetons se fait par l'intermédiaire de mineurs "Mining".Les jetons Watt sont émis linéairement.

(2) Consommation de l'utilisateur: l'utilisateur achète d'abord des jetons auprès des mineurs pour payer les frais de stockage et de trafic en utilisant le système watt.Les jetons circulent pour la première fois, des mineurs aux utilisateurs, reflétant la valeur de circulation des jetons watt.Les mineurs obtiennent le revenu final par l'intermédiaire des jetons.

2.Watt Economic Model

D'autre part, le système Watt tente de trouver un équilibre en créant un sentiment de rareté pour les pièces Watt tout en veillant à ce qu'un grand nombre de pièces Watt ne s'accumulent pas entre les mains d'un très petit nombre de personnes.Watt veut s'assurer que les utilisateurs de Watt obtiennent plus de jetons Watt lorsqu'ils contribuent au réseau.L'objectif est d'établir un modèle économique suffisamment complexe pour atteindre et équilibrer ces priorités,Tout en restant suffisamment intuitif pour que les gens puissent l'utiliser.Exigences de conception du modèle économique du Watt:

- simple: créer un modèle intuitif et transparent
- répartition équitable: accès à la Watt pour un nombre suffisant de personnes dans le monde
- Rareté: créer un sentiment de rareté pour maintenir les prix du Watt sans dévaluer avec le temps
- revenus d'élite: récompenser la contribution à la création et au maintien de réseaux

3.Schéma de distribution du Watt

Total: 20 milliards d'équipes réservées 5%

Phase 1: distribution gratuite de réseaux de croissance des utilisateurs basés sur l'application

La distribution totale au cours de la première phase n'est pas inférieure à 30% (6 milliards) de la distribution totale gratuite à l'intérieur de l'application, accumulant la population minière et la population consensuelle de stockage distribué, qui ne peuvent être obtenues gratuitement par la suite.Arrêter l'exploitation par consensus du SCP et la distribution gratuite jusqu'à la fin de l'exploitation minière de 6 milliards d'unités.

Phase II: réalisation de l'extraction sur disque dur, basée sur l'extraction de gage et l'extraction de stockage.

Dans le cas de la chaîne Watt, le noeud de validation est responsable de l'exploitation du réseau de consensus de l'élément principal watt. La récompense par bloc du réseau de consensus est la principale composante du système d'incitation économique de l'élément principal watt.Block Rewards Output watt.Après avoir reçu successivement des demandes commerciales, le watt payé pour l'espace de stockage est également un élément important du système d'incitation économique.La récompense du bloc principal Watt est principalement obtenue à partir de trois types d'exploitation minière: l'exploitation minière en gage et l'exploitation minière en stockage.

(1) Gage watt.Pour des raisons de stabilité économique, le TBB doit être mis en gage pour l'exploitation minière et l'exploitation minière de stockage.Dans l'état du lot Watt, le gage Watt est égal à 1 TB de droits miniers promis et 1 TB de droits miniers stockés.

(2) 2. Exploitation minière en gage.Par conséquent, les principaux éléments du gage sont le consensus et la sécurité. Tous les participants au système Watt ont besoin du gage Watt, et tous les nantissements recevront une récompense de bloc comme base d'incitation économique pour le consensus opérationnel.

(3) 3. Stockage et exploitation minière.Le stockage et l'exploitation minière sont la partie compétitive de l'état économique du Watt.La quantité totale d'exploitation minière au cours de la deuxième étape est temporairement incertaine.

Phase III:La troisième étape consiste à exploiter des équipements mobiles;

Sur la base de la deuxième phase de l'exploitation minière sur disque dur, un vaste pool de stockage interstellaire peut être construit en connectant des ressources de stockage mobiles dispersées à l'échelle mondiale pour assurer la souveraineté des données de tout le monde, avec une efficacité de stockage maximale, la fiabilité des données, la sécurité des données et Les coûts de stockage.Stocke et récupère l'exploitation minière à partir d'appareils mobiles et récompense.

IX.Gouvernance - crypto - monnaie créée et utilisée par le public

Pour élaborer un modèle de gouvernance durable, le watt mettra en oeuvre un plan en deux étapes.

1.Modèle de gouvernance provisoire (< 5m membres)

Le Watt fonctionnera selon un modèle de gouvernance provisoire jusqu'à ce que le réseau atteigne le nombre critique de membres de 5m.Le modèle ressemblera le plus au modèle de gouvernance « hors chaîne » actuellement utilisé par des protocoles comme filecoin et ethereum, et l'équipe centrale de Watt jouera un rôle important dans l'élaboration du Protocole.Toutefois, l'équipe de base du Watt continuera de s'appuyer

largement sur l'opinion de la communauté.L'équipe de base du Watt a consulté la communauté sur l'application mobile du Watt elle - même et a interagi avec les wattoniers.Watt accepte les critiques et les suggestions de la communauté, ce qui se fait par l'intermédiaire de la page d'atterrissage de Watt, de la FAQ et de la fonction de commentaires ouverts du Livre blanc.Chaque fois que les gens parcourent le site Web du Watt, ils peuvent soumettre des commentaires dans une section spécifique du site.Pour poser des questions et faire des recommandations.

De plus, l'équipe centrale du Watt élaborera des mécanismes de gouvernance plus formels.Un système de gouvernance potentiel est la démocratie mobile.Dans une démocratie mobile, chaque pionnier peut voter directement sur une question ou déléguer son droit de vote à d'autres membres du réseau.La démocratie mobile permettra à la communauté Watt d'avoir une adhésion large et efficace.

2.Convention constitutionnelle du Watt (> 5m membres)

Une fois qu'il aura atteint la composition du 5m, un comité intérimaire sera constitué sur la base des contributions antérieures au réseau watt.Le Comité sera chargé de consulter l'ensemble de la communauté et de formuler des recommandations.Il organisera également une série de conversations en ligne et hors ligne, et les membres du Watt seront en mesure d'évaluer la composition à long terme du Watt.Compte tenu de la base mondiale d'utilisateurs de Watt,Le réseau Watt exécutera ces conventions à plusieurs endroits dans le monde pour assurer l'accessibilité.En plus d'accueillir des réunions sur place, watt utilisera son application mobile comme plate - forme pour permettre aux membres de Watt de participer à distance au processus.Que ce soit en personne ou en ligne, les membres de la collectivité du Watt ont la capacité de participer à l'élaboration de la structure de gouvernance à long terme du Watt.

X.Feuille de route / plan de déploiement

Phase I - conception et distribution des guides miniers watt.

Développer l'application mobile pour l'exploitation minière SCP basée sur le plan de croissance des utilisateurs du réseau et l'agrégation de consensus, élargir la base de consensus pour le stockage mobile décentralisé, et développer le réseau principal. Utiliser l'algorithme de consensus stellaire SCP pour l'exploitation minière, et arrêter l'exploitation minière de consensus SCP lorsque l'exploitation minière atteint la fin de 6 milliards de pièces.

Phase II - réseau d'essai

Le logiciel de noeud de Watt sera déployé sur un réseau de test avant que nous commencions le réseau principal.Le réseau d'essai utilisera exactement la même carte de confiance que le réseau principal, mais sur le système de monnaie Watt d'essai.L'équipe de base hébergera plusieurs noeuds sur le réseau d'essai, mais encouragera d'autres pionniers à démarrer leurs propres noeuds sur le réseau d'essai.En fait,Afin de permettre à n'importe quel noeud de rejoindre le réseau principal, il est recommandé de commencer par le réseau d'essai.Le réseau d'essai fonctionnera en parallèle avec le

simulateur Watt au cours de la première phase et sera comparé périodiquement, par exemple quotidiennement, les résultats des deux systèmes seront comparés pour saisir les lacunes et les vulnérabilités du réseau d'essai, ce qui permettra aux développeurs Watt de faire des recommandations et de mettre en oeuvre des correctifs.Une fois que les deux systèmes fonctionnent complètement en parallèle, le réseau d'essai atteindra l'état où ses résultats sont conformes à ceux du simulateur.D'ici là, lorsque la communauté aura l'impression qu'elle est prête, watt passera à l'étape suivante, où Watt effectuera des essais miniers décentralisés en utilisant des preuves spatio - temporelles pour permettre à tout le monde de participer au stockage décentralisé.

Phase III - réseau principal

Lorsque la communauté estime que le logiciel est opérationnel et qu'il a été entièrement testé sur le réseau d'essai, le réseau principal officiel du réseau Watt est lancé.Un détail important est que lors de la transition vers le réseau principal, l'authentification des comptes sera effectuée pour s'assurer que chaque utilisateur est une personne réelle différente.Par la suite, le système de distribution de la phase 1 et le simulateur de réseau Watt seront fermés.Le système fonctionnera toujours seul.Les futures mises à jour de l'entente seront fournies par la communauté des développeurs de Watt et l'équipe de base de Watt et seront proposées par le Conseil.Leur mise en œuvre et leur déploiement dépendront de la mise à jour du logiciel minier par les noeuds, comme tout autre blockchain.Il n'y a pas d'organisme central qui contrôlera la monnaie et elle sera entièrement distribuée.Les soldes des utilisateurs fictifs ou dupliqués seront supprimés.À ce stade, watt se connectera à la bourse et négociera avec d'autres devises.