Pi Network Whitepaper

PLAN

Ébauche 1 du 14 mars 2019 traduction du 16 Août 2019

PREFACE

Alors que le monde devient de plus en plus numérique, la cryptomonnaie est une nouvelle étape naturelle dans l'évolution de la monnaie. Pi est la première monnaie numérique pour gens ordinaires, ce qui représente un grand pas en avant dans l'adoption de la cryptomonnaie dans le monde entier.

Notre mission : Créer une plate-forme de cryptomonnaie et de contrats intelligents sécurisée et exploitée par des personnes ordinaires.

Notre vision : Construire le marché peer-to-peer le plus inclusif du monde, alimenté par Pi, la cryptomonnaie la plus utilisée au monde.

AVERTISSEMENT pour les lecteurs plus avancés : Parce que la mission de Pi est d'être le plus inclusif possible, nous allons profiter de l'occasion pour présenter à nos débutants de la blockchain les fondamentaux .

INTRODUCTION : Pourquoi les cryptomonnaies sont-elles importantes ?

À l'heure actuelle, nos opérations financières courantes reposent sur un ***tiers de confiance*** qui tient un registre des opérations. Par exemple, lorsque vous effectuez une transaction bancaire, le système bancaire tient un registre et garantit que la transaction est sûre et fiable. De même, lorsque Cindy transfère 5 $ à Steve en utilisant PayPal, PayPal tient un registre central de 5 $ débités du compte de Cindy et de 5 $ crédités à celui de Steve. Les intermédiaires comme les banques, PayPal et d'autres membres du système économique actuel jouent un rôle important dans le contrôle et la réglementation des transactions financières mondiales.

Toutefois, le rôle de ces intermédiaires de confiance a aussi ses limites :

Captation indue de valeur : Ces intermédiaires amassent des milliards de dollars en création de richesse (la capitalisation boursière de PayPal est d'environ 130 milliards de dollars), mais n'en rétrocèdent pratiquement rien à leurs clients , les gens ordinaires sur le terrain, dont l'argent constitue une part importante de l'économie mondiale. De plus en plus de gens sont laissés pour compte.

Honoraires : Banques et entreprises prélèvent des frais importants pour opérer les transactions. Ces frais ont souvent un impact disproportionné sur les populations à faible revenu qui ont le moins d'alternatives.

La Censure : Si un ***tiers de confiance*** juge que vous ne devriez pas être en mesure de transférer votre argent, il peut imposer des restrictions sur le mouvement de votre argent.

Droit d'Autorisation : L'intermédiaire de confiance sert de gardien qui peut arbitrairement empêcher quiconque de faire partie du réseau.

Confidentialité : À une époque où la question de la protection de la vie privée devient de plus en plus urgente, ces puissants gardiens peuvent récupérer plus de renseignements financiers à votre sujet que vous ne le souhaiteriez, et, "accidentellement", les divulguer ou vous pousser à les divulguer.

Le "peer-to-peer electronic cash system" (système de paiement électronique point à point) de Bitcoin, lancé en 2009 par un programmeur (ou groupe) anonyme "Satoshi Nakamoto", a été un moment décisif pour la liberation de l'argent. Pour la première fois dans l'histoire, les gens pouvaient échanger de la valeur en toute sécurité, sans avoir recours à un tiers ou à un intermédiaire de confiance. En payant en Bitcoin, des gens comme Steve et Cindy pouvaient se payer directement l'un l'autre, en contournant les frais institutionnels, les obstructions et les intrusions. Bitcoin était vraiment une monnaie sans frontières, alimentant et connectant une nouvelle économie mondiale.

Introduction aux Registres distribués :

Bitcoin a réalisé cet exploit historique en utilisant l'enregistrement distribué de chaque évènement ou transaction. Alors que le système financier actuel repose sur l'enregistrement central traditionnel de la vérité, l'enregistrement Bitcoin est garanti et maintenu par une communauté distribuée de "validateurs", qui accèdent et mettent à jour ce grand livre (Registre) public. Imaginez le protocole Bitcoin comme un "Google Sheet" mondialement partagé qui contient les enregistrements validés des transactions, et maintenu par cette communauté distribuée.

La percée de Bitcoin (et de la technologie générale de la chaîne de blocks = Blockchain) est que, même si l'enregistrement est maintenu par une communauté, la technologie leur permet de toujours parvenir à un consensus sur les transactions authentiques, garantissant que les tricheurs ne peuvent pas enregistrer de fausses transactions ou contourner le système. Cette avancée technologique permet de supprimer l'intermédiaire centralisé, sans compromettre la sécurité financière transactionnelle.

Avantages des Registres répartis :
En plus de la décentralisation, le bitcoin, ou les cryptomonnaies en général, partagent quelques belles particularités qui rendent l'argent plus intelligent et plus sûr, même si différentes cryptomonnaies peuvent être plus fortes pour certaines propriétés et plus faibles pour d'autres, en fonction des différentes implémentations de leurs protocoles. Les cryptomonnaies sont conservées dans des “portefeuilles” numériques virtuels cryptés et identifiés par une adresse accessible au public, et sont protégés par un mot de passe privé très solide, appelé clé privée. Cette clé privée signe cryptographiquement la transaction et il est pratiquement impossible de créer des signatures frauduleuses. Cela assure la sécurité et l'insaisissabilité. Contrairement aux comptes bancaires traditionnels qui peuvent être saisis par les autorités gouvernementales, l’accès à votre portefeuille est absolument impossible à quiconque sans votre clé privée. Les cryptomonnaies résistent à la censure en raison de leur nature décentralisée, car n'importe qui peut soumettre des transactions à n'importe quel ordinateur du réseau pour être enregistrées et validées. Les transactions en cryptomonnaie sont immuables et inaltérables car chaque bloc de transactions représente une preuve cryptographique (un hachage) de tous les blocs précédents qui existaient avant lui. Si quelqu'un vous envoie de l'argent, il ne peut pas annuler son paiement (c.-à-d., pas de chèques sans provision dans la Blockchain). Les " contrats intelligents " construits sur ces cryptomonnaies ne reposent pas seulement sur l'application de la loi, mais sont directement appliqués par le biais d'un code publiquement contrôlable, ce qui les rend inviolables et peut potentiellement éliminer les intermédiaires dans de nombreuses entreprises, par exemple les dépôts de garantie, cautions et/ou sequestre en matière immobilière.

Sécurisation des Registres distribués (Minage) : Dans le cas du BITCOIN :
L'un des défis que pose la tenue d'un registre réparti des transactions est la sécurité :
Comment avoir un registre ouvert et modifiable tout en prévenant les activités frauduleuses.
Pour relever ce défi, Bitcoin a introduit un nouveau processus appelé Mining (utilisant l'algorithme consensuel "Proof of Work") pour déterminer à qui l'on fait "confiance" pour effectuer les mises à jour des enregistrements partagés des transactions et la validation de nouveaux enregistrements.

On peut considérer le **Minage** comme une sorte de jeu économique qui oblige les "validateurs" à prouver leur mérite lorsqu'ils tentent d'ajouter des transactions au Registre. Pour se qualifier, les validateurs doivent résoudre une série de puzzles informatiques complexes. Le validateur qui résout le puzzle le premier est récompensé en étant autorisé à poster le dernier bloc de transactions. L'affichage du dernier bloc de transactions permet au validateur de recevoir une récompense/rémunération sous forme de “Token” (ou “ Coin “) - actuellement 12,5 bitcoin (~ 115 000 € à mi-Août 2019).

Ce processus est très sûr, mais il exige une puissance de calcul et une consommation d'énergie énormes car les validateurs "brûlent de l'argent" pour résoudre le puzzle informatique qui leur rapporte plus de bitcoin. Le ratio brûlure/récompense est si punitif qu'il est toujours dans l'intérêt des validateurs d'afficher des transactions honnêtes dans le dossier Bitcoin.

PROBLEME : Concentration du pouvoir et de l'argent .

Les cryptomonnaies de 1ère génération deviennent hors de portée.

Dans les premiers temps de Bitcoin, alors que peu de personnes travaillaient à valider les transactions et à extraire les premiers blocs, n'importe qui pouvait gagner 50 BTC en exécutant simplement le logiciel d'extraction Bitcoin sur son ordinateur personnel. Au fur et à mesure que la monnaie a commencé à gagner en popularité, des mineurs intelligents ont réalisé qu'ils pouvaient gagner plus s'ils exploitaient plus d'un ordinateur.

Au fur et à mesure que la valeur de Bitcoin continuait d'augmenter, des entreprises entières de “Minage”ont commencé à se développer. Ces sociétés utilisent des puces spécialisées (" ASIC ") et ont construit d'énormes fermes de serveurs utilisant ces puces ASIC pour miner des Bitcoin. L'émergence de ces énormes sociétés minières, connues pour être à l'origine de la ruée vers l'or Bitcoin, a rendu très difficile pour les gens ordinaires de participer au minage et d'être récompensés. Les fermes de minage ont également commencé à consommer des quantités de plus en plus importantes d'énergie électrique et informatique, ce qui a contribué à accroître les problèmes environnementaux dans le monde entier.

La facilité d'exploitation de Bitcoin et la montée en puissance des fermes de minage de Bitcoin ont rapidement conduit à une centralisation massive du pouvoir de production et de la richesse dans le réseau de Bitcoin. Pour donner une idée, 87% de tous les bitcoins sont aujourd’hui détenus par 1% des détenteurs de “wallets” (portefeuilles), beaucoup de ces pièces ont été minées pratiquement gratuitement dans leurs premiers jours; autre illustration, Bitmain, l'une des plus grandes exploitations de minage de Bitcoin, a généré des milliards de dollars de revenus et de profits.

La centralisation du pouvoir dans le réseau de Bitcoin le rend très difficile et coûteux pour la personne moyenne. Si vous voulez acquérir du Bitcoin, vos options les plus simples sont de :

Miner vous-même : Il suffit de brancher le matériel spécialisé (lien sur Amazon) . Sachez juste que puisque vous serez en compétition avec d'énormes fermes de serveurs du monde entier, consommant autant d'énergie que la Suisse, vous ne serez pas en mesure d'en exploiter beaucoup.

Acheter Bitcoin sur une plateforme d’échange. Aujourd'hui, vous pouvez acheter Bitcoin au prix unitaire de 9000 € la pièce au 15/08/2019 (note : vous pouvez acheter une fraction de Bitcoin !) Bien sûr, vous prendriez aussi un risque important en le faisant car le prix du Bitcoin est très volatile.

Bitcoin a été le premier à montrer comment la cryptomonnaie pouvait perturber le modèle financier actuel, donnant aux gens la possibilité d'effectuer des transactions sans l'intervention d'un tiers. L'accroissement de la liberté, de la flexibilité et de la protection de la vie privée continue d'entretenir l'inévitable marche vers les monnaies numériques en tant que nouvelle norme. Malgré ses avantages pour certains, la concentration (probablement involontaire) de l'argent et du pouvoir de Bitcoin constitue un obstacle important à son adoption par le grand public.
L'équipe centrale de Pi (Pi-Core-Team) a mené des recherches pour comprendre pourquoi les gens sont réticents à entrer dans l'univers des cryptomonnaies. Les gens ont toujours mentionné le risque d'investissement ou d'exploitation minière comme étant un obstacle majeur à l'entrée sur le marché.

SOLUTION : Pi - Activation du minage sur les téléphones mobiles
Après avoir identifié ces principaux obstacles à l'adoption, l'équipe Pi Core s'est mise en quête d'un moyen de permettre aux gens ordinaires d'exploiter (ou de gagner des récompenses en cryptomonnaie pour avoir validé des transactions sur un enregistrement distribué des transactions). Pour rappel, l'un des principaux défis que pose la tenue d'un registre réparti des transactions est de s'assurer que les mises à jour de ce registre ouvert ne sont pas frauduleuses. Bien que le processus de Bitcoin pour la mise à jour de son dossier soit éprouvé (brûler de l'énergie/argent pour prouver sa fiabilité), il n'est pas très convivial pour l'utilisateur (ou la planète !). Pour Pi, nous avons introduit l'exigence de conception supplémentaire d'employer un algorithme de consensus qui serait également extrêmement convivial et qui permettrait idéalement le minage sur les ordinateurs personnels et les téléphones mobiles.

En comparant les algorithmes de consensus existants (le processus qui fiabilise et enregistre les transactions dans un registre distribué), le Stellar Consensus Protocol apparaît comme le principal candidat pour permettre un minage convivial et mobile. **Stellar Consensus Protocol (SCP)** a été conçu par David Mazières, professeur d'informatique à Stanford et scientifique en chef à la Stellar Development Foundation. SCP utilise un nouveau mécanisme appelé "**Accords Byzantins Fédérés"** pour s'assurer que les mises à jour d'un registre ou grand livre distribué sont exactes et fiables. Le SCP est également déployé dans la pratique par le biais de la chaîne stellaire qui est opérationnelle depuis 2015.

****

<u>Introduction simplifiée aux algorithmes de consensus</u>
Avant de passer à l'introduction de l'algorithme de consensus Pi, il est utile d'avoir une explication simple de ce que fait un algorithme de consensus pour une chaîne de blocs et des types d'algorithmes de consensus que les protocoles actuels de chaînes de blocs utilisent généralement, par exemple, Bitcoin et SCP. Dans un souci de clarté, cette section est explicitement rédigée d'une manière trop simplifiée et n'est pas complète. Pour une plus grande précision, voir la section Adaptations à la SCP ci-dessous et lire le document du Protocole de Consensus Stellar (SCP).

Une chaîne de blocs est un système distribué à tolérance de pannes qui vise à ordonner totalement une liste de blocs de transactions. Les systèmes distribués à tolérance de pannes sont un domaine de l'informatique qui a été étudié pendant de nombreuses décennies. On les appelle systèmes distribués parce qu'ils n'ont pas de serveur centralisé mais plutôt une liste décentralisée d'ordinateurs (appelés nœuds ou pairs) qui doivent parvenir à un consensus quant au contenu et à l'ordre total des blocs. Ils sont également appelés tolérants aux pannes parce qu'ils peuvent tolérer un certain degré de nœuds défectueux dans le système (par exemple, jusqu'à 33 % des nœuds peuvent être défectueux et l'ensemble du système continue à fonctionner normalement).

Il existe deux grandes catégories d'algorithmes de consensus : Ceux qui élisent un nœud comme chef qui produit le bloc suivant, et ceux où il n'y a pas de chef explicite mais où tous les nœuds parviennent à un consensus sur ce que sera le bloc suivant après avoir échangé des votes en s'envoyant des messages informatiques. (Strictement parlant, cette dernière phrase contient de multiples inexactitudes, mais elle nous aide à expliquer les grandes lignes.)

Bitcoin utilise le premier type d'algorithme de consensus : Tous les nœuds bitcoin sont en compétition pour résoudre un puzzle cryptographique. Parce que la solution est trouvée au hasard, essentiellement le nœud qui trouve la solution le premier, par hasard, est élu chef de file de la ronde qui produit le bloc suivant. Cet algorithme s'appelle "Preuve de travail" et entraîne une forte consommation d'énergie.

INTRODUCTION simplifiée au Protocole de Consensus Stellar (SCP)

Pi utilise l'autre type d'algorithmes de consensus et est basé sur le Protocole de Consensus Stellar (SCP) et un algorithme appelé **Federated Byzantine Agreement** (**FBA**). De tels algorithmes n'ont pas de gaspillage d'énergie, mais ils nécessitent l'échange de nombreux messages réseau afin que les nœuds parviennent à un "consensus" sur ce que devrait être le bloc suivant. Chaque nœud peut déterminer indépendamment si une transaction est valide ou non, par exemple l'autorisation d'effectuer la transition et la double dépense, en fonction de la signature cryptographique et de l'historique des transactions. Toutefois, pour qu'un réseau d'ordinateurs s'entende sur les transactions à enregistrer dans un bloc et sur l'ordre de ces transactions et de ces blocs, il faut qu'ils se transmettent des messages et disposent de plusieurs tours de scrutin pour parvenir à un consensus. Intuitivement, de tels messages provenant de différents ordinateurs du réseau et concernant quel bloc est le suivant ressembleraient à ce qui suit : "Je propose que nous votions tous pour que le bloc A soit le prochain bloc " ; " Je vote pour que le bloc A soit le bloc suivant " ; " Je confirme que la majorité des noeuds en qui j'ai confiance ont également voté pour le bloc A ", dont l'algorithme de consensus permet à ce noeud de conclure que " A est le bloc suivant ; et il ne pourrait y avoir aucun bloc autre que A comme bloc suivant " ; Même si les étapes ci-dessus semblent nombreuses, Internet est suffisamment rapide et ces messages sont légers, donc ces algorithmes sont plus légers que la validation de Bitcoin par la preuve de travail (Proof of Work). L'un des principaux représentants de ces algorithmes est appelé Tolérance de Faute Byzantine (BFT). Plusieurs des chaînes de blocs les plus importantes aujourd'hui sont basées sur des variantes de BFT, telles que NEO et Ripple.

L'une des principales critiques à l'égard de la BFT est qu'elle a un point de centralisation : parce qu'il s'agit d'un vote, l'ensemble des nœuds participant au "quorum" du vote est déterminé de manière centralisée par le créateur du système à ses débuts. La contribution de la FBA est qu'au lieu d'avoir un quorum déterminé de manière centralisée, chaque nœud fixe ses propres "tranches de quorum", qui formeront à leur tour des quorums différents. De nouveaux nœuds peuvent rejoindre le réseau de manière décentralisée : ils déclarent les nœuds en qui ils ont confiance et convainquent les autres nœuds de leur faire confiance, mais ils n'ont pas besoin de convaincre une autorité centrale.

SCP est une instanciation de FBA. Au lieu de brûler de l'énergie comme dans l'algorithme de consensus de preuve de travail de Bitcoin, les nœuds SCP sécurisent l'enregistrement partagé en se portant garants de la fiabilité des autres nœuds du réseau. Chaque nœud du réseau constitue une tranche de quorum,

constituée d'autres nœuds du réseau qu'ils jugent dignes de confiance. Les quorums sont formés sur la base des tranches de quorum de ses membres, et un validateur n'acceptera de nouvelles transactions que si et seulement si une proportion de nœuds dans leurs quorums acceptera également la transaction. Comme les validateurs du réseau construisent leurs quorums, ces quorums aident les nœuds à atteindre un consensus sur les transactions avec garantie de sécurité. Vous pouvez en apprendre davantage sur le Protocole de Consensus Stellar (SCP) en regardant cette courte vidéo d'explication de 7 minutes ou en consultant ce résumé technique du SCP.

ADAPTATIONS de Pi au Protocole de Consensus Stellaire (SCP)

L'algorithme de consensus de Pi se construit au dessus de SCP. Le SCP a été formellement prouvé [Mazieres 2015] et est actuellement mis en œuvre au sein du réseau Stellar. Contrairement à Stellar Network qui se compose principalement d'entreprises et d'institutions (par exemple, IBM) en tant que nœuds, Pi a l'intention de permettre aux équipements individuels de contribuer au niveau du protocole et d'être récompensé, y compris les téléphones mobiles, ordinateurs portables et ordinateurs. Vous trouverez ci-dessous une introduction sur la façon dont Pi applique le SCP pour permettre l'exploitation minière par les particuliers.

Les utilisateurs de Pi peuvent jouer quatre rôles en tant que mineurs Pi. A savoir :

- **Pionnier :** Un utilisateur de l'application mobile Pi qui confirme simplement qu'il n'est pas un "robot" au quotidien. Cet utilisateur valide sa présence à chaque fois qu'il se connecte à l'application. Il peut également ouvrir l'application pour demander des transactions (par exemple, effectuer un paiement en Pi à un autre Pionnier).
- **Contributeur :** Un utilisateur de l'application mobile Pi qui contribue en fournissant une liste de pionniers qu'il ou elle connaît et en qui il ou elle a confiance. Dans leur ensemble, les contributeurs Pi construiront un graphique global de confiance.
- **Ambassadeur :** Un utilisateur de l'application mobile Pi qui introduit d'autres utilisateurs dans le réseau Pi.
- **Nœud (node) :** Un utilisateur qui est un pionnier, un contributeur utilisant l'application mobile Pi, et qui exécute également le logiciel du nœud Pi sur son ordinateur de bureau ou portable. Le logiciel du nœud Pi est le logiciel qui exécute l'algorithme SCP de base, en tenant compte des informations du graphique de confiance fournies par les contributeurs.

Un utilisateur peut jouer plus d'un des rôles ci-dessus. Tous les rôles sont nécessaires, donc tous les rôles sont récompensés par des Pi nouvellement frappés sur une base quotidienne tant qu'ils ont participé et contribué pendant cette journée donnée. Dans la définition vague d'un "mineur" qui est un utilisateur qui reçoit de la monnaie nouvellement frappée comme récompense pour ses contributions, les quatre rôles sont considérés comme des mineurs Pi. Nous définissons le terme " minage " de façon plus large que son sens traditionnel qui équivaut à l'exécution d'un algorithme consensuel de preuve du travail, comme dans Bitcoin ou Ethereum.

Tout d'abord, il faut souligner que le logiciel Pi Node n'est pas encore sorti. Cette section est donc davantage offerte en tant que conception architecturale et en tant que demande de commentaires de la part de la communauté technique. Ce logiciel sera entièrement open source et dépendra aussi fortement de stellar-core qui est aussi un logiciel open source, disponible ici. Cela signifie que n'importe qui dans la communauté pourra lire, commenter et proposer des améliorations. Ci-dessous se trouvent les changements proposés par Pi à la MCS pour permettre l'exploitation minière à l'aide d'appareils individuels.

Nœuds

Pour une bonne lisibilité, nous définissons comme un nœud correctement connecté ce que le document SCP appelle un nœud intact. De même nous définissons comme le réseau principal Pi l'ensemble de tous les nœuds intacts du réseau Pi. La tâche principale de chaque Nœud est d'être configuré pour être correctement connecté au réseau principal Pi. Intuitivement, un nœud mal connecté au réseau principal est similaire à un nœud Bitcoin non connecté au réseau principal bitcoin.

En termes de SCP, pour qu'un nœud soit correctement connecté, ce nœud doit choisir une "tranche de quorum" de sorte que tous les quorums résultants qui incluent ce nœud se recoupent avec les quorums du réseau existant. Plus précisément, un nœud vn+1 est correctement connecté à un réseau principal N de n nœuds déjà correctement connectés (v1, v2, ..., vn) si le système résultant N' de n+1 nœuds (v1, v2, ..., vn+1) bénéficie d'une intersection du quorum. En d'autres termes, N' jouit de l'intersection du quorum si deux de ses quorums partagent un nœud. -- Pour tous les quorums U1 et U2, $U1 \cap U2 \neq \neq \emptyset$.

La principale contribution de Pi par rapport au déploiement par consensus Stellar existant est qu'il introduit le concept d'un graphique de confiance fourni par les contributeurs Pi comme information pouvant être utilisée par les nœuds Pi lorsqu'ils configurent leurs configurations pour se connecter au réseau Pi principal.

Lorsqu'ils choisissent leurs tranches de quorum, ces nœuds doivent tenir compte du graphique de confiance fourni par les contributeurs, y compris leur propre cercle de sécurité. Pour faciliter cette décision, nous avons l'intention de fournir un logiciel auxiliaire d'analyse graphique pour aider les utilisateurs qui utilisent Nodes à prendre des décisions aussi éclairées que possible. La production quotidienne de ce logiciel comprendra :

- un classement des nœuds en fonction de leur distance par rapport au nœud actuel dans le graphique de confiance ; un classement des nœuds basé sur une analyse de pagerank des nœuds dans le graphique de confiance ,

- une liste des nœuds signalés par la communauté comme défectueux de quelque manière que ce soit et une liste des nouveaux nœuds cherchant à rejoindre le réseau ,

- une liste des articles les plus récents du web sur le mot-clé " mauvais comportement des nœuds Pi " et d'autres mots-clés associés ; une représentation visuelle des Nœuds composant le réseau Pi similaire à ce qui est affiché dans le moniteur StellarBeat Quorum[code source].

- un explorateur de quorum similaire à QuorumExplorer.com[code source].

- un outil de simulation comme celui du moniteur StellarBeat Quorum qui montre les impacts attendus sur la connectivité de ces nœuds au réseau Pi lorsque la configuration du nœud actuel change.

Un sujet de recherche intéressant pour les travaux futurs sera de développer des algorithmes qui peuvent prendre en compte le graphique de confiance et suggérer à chaque nœud une configuration optimale, ou même définir cette configuration automatiquement. Lors du premier déploiement du réseau Pi, alors que les utilisateurs exécutant des nœuds peuvent mettre à jour leur configuration de nœud à tout moment, ils seront invités à confirmer leurs configurations quotidiennement et à les mettre à jour s'ils le souhaitent.

Utilisateurs d'applications mobiles

Lorsqu'un Pioneer doit confirmer qu'une transaction donnée a été exécutée (par exemple, qu'il a reçu Pi), il ouvre l'application mobile. À ce moment-là, l'application mobile se connecte à un ou plusieurs nœuds pour savoir si la transaction a été enregistrée dans le grand livre et aussi pour obtenir le numéro de bloc le plus récent et la valeur de hachage de ce bloc. Si ce Pioneer exploite également un nœud, l'application mobile se connecte au nœud de ce Pioneer. Si le Pioneer n'exécute pas de nœud, l'application se connecte à plusieurs nœuds et vérifie ces informations. Les pionniers auront la possibilité de choisir les nœuds auxquels ils veulent que leurs applications se connectent. Mais pour simplifier les choses pour la plupart des utilisateurs, l'application devrait avoir un ensemble raisonnable de nœuds par défaut, par exemple un certain nombre de nœuds les plus proches de l'utilisateur sur la base du graphique de confiance, ainsi qu'une sélection aléatoire de nœuds ayant un rang élevé. Nous vous demandons votre avis sur la façon dont le jeu de nœuds par défaut pour les Pionniers mobiles devrait être sélectionné.

Récompenses de minage

Une belle propriété de l'algorithme SCP est qu'il est plus générique qu'une chaîne de blocs. Il coordonne le consensus au sein d'un système réparti de nœuds. Cela signifie que le même algorithme de base n'est pas seulement utilisé toutes les quelques secondes pour enregistrer de nouvelles transactions dans de nouveaux blocs, mais qu'il peut également être utilisé pour exécuter périodiquement des calculs plus complexes. Par exemple, une fois par semaine, le réseau Stellar l'utilise pour calculer l'inflation sur le réseau Stellar et allouer les jetons nouvellement frappés proportionnellement à tous les supports de pièces Stellar (la pièce de monnaie Stellar s'appelle Lumen). De la même manière, le réseau Pi emploie SCP une fois par jour pour calculer la nouvelle distribution de Pi dans l'ensemble du réseau parmi tous les mineurs Pi (pionniers, collaborateurs, ambassadeurs, nœuds) qui ont participé activement à une journée donnée. En d'autres termes, les récompenses de minage de Pi ne sont calculées qu'une fois par jour et non sur chaque bloc de la chaîne de blocs.

A titre de comparaison, Bitcoin attribue des récompenses minières sur chaque bloc et donne toute la récompense au mineur qui a eu la chance d'être capable de résoudre une tâche randomisée intensive en calcul. Cette récompense en Bitcoin actuellement 12.5 Bitcoin (~115K€) est donnée à un seul mineur toutes les 10 minutes. Il est donc extrêmement improbable qu'un mineur puisse jamais être récompensé. Comme solution à cela, les mineurs de bitcoin s'organisent en pools de minage centralisés, qui contribuent tous à la puissance de traitement, ce qui augmente la probabilité d'obtenir des récompenses

et, éventuellement, de partager proportionnellement ces récompenses. Les gisements miniers ne sont pas seulement des points de centralisation, mais leurs exploitants obtiennent également des réductions qui réduisent le montant alloué aux mineurs individuels. En Pi, il n'y a pas besoin de tels pools, car une fois par jour, tous ceux qui ont contribué reçoivent une distribution méritocratique de nouveaux Pi.

Frais de transaction

Comme pour les transactions Bitcoin, les frais sont facultatifs dans le réseau Pi. Chaque bloc a une certaine limite quant au nombre de transactions qu'il peut contenir. Lorsqu'il n'y a pas d'arriéré de transactions, les transactions ont tendance à être gratuites. Mais s'il y a plus de transactions, les nœuds les classent en fonction des frais, avec les transactions les plus élevées en tête de liste et ne choisissent que les transactions les plus importantes à inclure dans les blocs produits. Cela en fait un marché ouvert. Mise en œuvre : Les frais sont répartis proportionnellement entre les nœuds une fois par jour. Sur chaque bloc, les frais de chaque transaction sont transférés dans un portefeuille temporaire d'où ils sont distribués aux mineurs actifs de la journée. Ce portefeuille a une clé privée inconnue. Les transactions à l'intérieur et à l'extérieur de ce portefeuille sont forcées par le protocole lui-même sous le consensus de tous les nœuds de la même manière que le consensus crée de nouveaux Pi chaque jour.

Limites et travaux futurs

SCP a été largement testé pendant plusieurs années dans le cadre du réseau Stellar qui, au moment de la rédaction de cet article, est la neuvième plus grande cryptomonnaie au monde. Cela nous donne une assez grande confiance en elle. L'une des ambitions du projet Pi est de faire en sorte que le nombre de nœuds du réseau Pi soit supérieur au nombre de nœuds du réseau Stellar pour permettre à un plus grand nombre d'utilisateurs quotidiens de participer à l'algorithme de consensus central. L'augmentation du nombre de nœuds augmentera inévitablement le nombre de messages réseau qui doivent être échangés entre eux. Même si ces messages sont beaucoup plus petits qu'une image ou qu'une vidéo sur Youtube et qu'Internet peut aujourd'hui transférer des vidéos de manière fiable et rapide, le nombre de messages nécessaires augmente avec le nombre de nœuds participants, ce qui peut devenir un goulot d'étranglement pour atteindre rapidement le consensus. Cela finira par ralentir le rythme auquel les nouveaux blocs et les nouvelles transactions sont enregistrés sur le réseau. Heureusement, Stellar est actuellement beaucoup plus rapide que Bitcoin. Actuellement, Stellar est calibré pour produire un nouveau bloc toutes les 3 à 5 secondes, pouvant supporter des milliers de transactions par seconde. Par comparaison, Bitcoin produit un nouveau bloc toutes les 10 minutes. De plus, en raison de l'absence de garantie de sécurité de Bitcoin, la Blockchain de Bitcoin peut, en de rares occasions, être écrasée dans la première heure. Cela signifie qu'un utilisateur de Bitcoin doit attendre environ 1 heure avant de pouvoir être sûr qu'une transaction est considérée comme définitive. SCP garantit la sécurité, ce qui signifie qu'après 3 à 5 secondes, on est certain d'une transaction. Ainsi, même avec le goulot d'étranglement potentiel de l'extensibilité, Pi s'attend à réaliser la finalité de la transaction plus rapidement que Bitcoin et peut-être plus lentement que Stellar, et à traiter plus de transactions par seconde que Bitcoin et peut-être moins que Stellar.

Bien que l'extensibilité des SCP demeure un problème de recherche ouvert. Il y a de multiples façons prometteuses d'accélérer les choses. Une solution d'évolutivité possible est bloXroute. BloXroute propose un réseau de distribution de chaînes de blocs (BDN = Blockchain Distribution Network) qui utilise un réseau mondial de serveurs optimisés pour la performance du réseau. Bien que chaque BDN

soit contrôlé de façon centralisée par une seule organisation, il offre une accélération de passage de message manifestement neutre. C'est-à-dire que les BDN ne peuvent desservir tous les nœuds que de manière équitable et sans discrimination puisque les messages sont cryptés. Cela signifie que le BDN ne sait pas d'où viennent les messages, où ils vont ou ce qu'il contient. De cette façon, les nœuds Pi peuvent avoir deux routes de passage de messages : Un rapide à travers BDN, qui devrait être fiable la plupart du temps, et son interface originale de passage de message peer-to-peer qui est entièrement décentralisée et fiable mais qui est plus lente. L'intuition de cette idée est vaguement similaire à celle de la mise en cache : le cache est un endroit où un ordinateur peut accéder aux données très rapidement, ce qui accélère le calcul moyen, mais il n'est pas garanti d'avoir toujours toutes les informations nécessaires. Lorsque la mémoire cache manque, l'ordinateur est ralenti, mais rien de catastrophique ne se produit. Une autre solution peut consister à utiliser l'acquittement sécurisé des messages multicast dans les réseaux ouverts Peer-to-Peer[Nicolosi et Mazieres 2004] pour accélérer la propagation des messages entre pairs.

****

MODELE ECONOMIQUE DE Pi : Équilibrer la rareté et l'accès

Avantages et inconvénients des modèles économiques de première génération
L'une des innovations les plus impressionnantes de Bitcoin est son mariage des systèmes distribués et de la théorie des jeux économiques.

Avantages
Alimentation fixe
Le modèle économique de Bitcoin est simple. Il n'y aura jamais que 21 millions de Bitcoin en existence. Ce est nombre fait partie du code de Bitcoin. Avec seulement 21 millions de Bitcoins pour circuler parmi 7,5 milliards de personnes dans le monde, il n'y a pas assez de Bitcoin pour tout le monde. Cette rareté est l'un des facteurs les plus importants de la valeur de Bitcoin (mais l'utilisation des sous-multiples à grande échelle tels "Satoshi" atténue cet aspect).

Diminution de la prime de blocage
Le schéma de distribution de Bitcoin, illustré ci-dessous, renforce encore ce sentiment de rareté. La récompense pour l'exploitation minière des blocs de Bitcoin est divisée par deux tous les 210 000 blocs (environ tous les ~4 ans.) A ses débuts, la récompense pour les blocs de Bitcoin était de 50 pièces. Aujourd'hui, la récompense est de 12,5, et diminuera encore à 6,25 pièces en mai 2020. Le taux de distribution décroissant de Bitcoin signifie que, même si la notoriété de la monnaie augmente, il y en a de moins en moins à miner.

Inconvénients
Moyens inversés / Moyens inégaux
Le modèle de distribution inversée de Bitcoin (moins de personnes gagnant plus au début et plus de personnes gagnant moins aujourd'hui) est l'un des principaux facteurs contribuant à sa distribution inégale. Avec tant de Bitcoin entre les mains de quelques pionniers, les nouveaux mineurs "brûlent" plus d'énergie pour moins de bitcoin.

La thésaurisation empêche l'utilisation comme moyen d'échange
Bien que Bitcoin ait été lancé en tant que système "peer to peer electronic cash", la rareté relative de Bitcoin a empêché Bitcoin d'atteindre son objectif de servir de moyen d'échange. La rareté du bitcoin a conduit à sa perception comme une forme d'"or numérique" ou une réserve de valeur numérique. Le résultat de cette perception est que de nombreux détenteurs de Bitcoin ne sont pas disposés à dépenser Bitcoin pour leurs dépenses quotidiennes.

Le modèle économique Pi

Pi, d'autre part, cherche à trouver un équilibre entre la création d'un sentiment de rareté pour Pi, tout en veillant à ce qu'une grande quantité ne s'accumule pas dans un très petit nombre de mains. Nous voulons nous assurer que nos utilisateurs gagnent plus de Pi au fur et à mesure qu'ils contribuent au réseau. L'objectif de Pi est de construire un modèle économique suffisamment sophistiqué pour atteindre et équilibrer ces priorités tout en restant suffisamment intuitif pour que les gens puissent l'utiliser.
Pi en matière de conception de modèles économiques :
- Simple : Construire un modèle intuitif et transparent
- Répartition équitable : Donner à une masse critique de la population mondiale l'accès à Pi
- Pénurie : Créer un sentiment de rareté pour soutenir le prix de Pi dans le temps
- Gains méritocratiques : Récompenser les contributions pour bâtir et soutenir le réseau
- Pi - Jeton d'approvisionnement

- Politique en matière d'émissions de jetons :
Approvisionnement maximal total = M + R + R + D
M = récompenses minières totales
R = récompenses totales de référence
D = rémunération totale du développeur

$M = \int f(P)\,dx$ où f est une fonction logarithmique décroissante
P = Nombre de personnes (p. ex. 1re personne à joindre, 2e personne à joindre, etc.)
R = r * M r = taux de recommandation (50 % au total ou 25 % à la fois pour le référent et le référent)
D = t * (M + R) t = taux de récompense des promoteurs (25 %)

M - Approvisionnement de minage (basé sur l'offre de minage fixe frappée par personne)
Contrairement à Bitcoin qui a créé une réserve fixe de pièces pour l'ensemble de la population mondiale, Pi crée une réserve fixe de Pi pour chaque personne qui rejoint le réseau jusqu'aux 100 premiers millions de participants. En d'autres termes, pour chaque personne qui rejoint le réseau Pi, un montant fixe de Pi est préimprimé. Cet approvisionnement est ensuite réparti sur la durée de vie de ce membre en fonction de son niveau d'engagement et de sa contribution à la sécurité du réseau. L'approvisionnement est libéré à l'aide d'une fonction de décroissance exponentielle similaire à celle de Bitcoin au cours de la vie du membre.

R – Primes de Parrainage (basée sur une récompense de parrainage fixe frappée par personne et partagée avec un parrain et un filleul)
Pour qu'une monnaie ait de la valeur, elle doit être largement distribuée. Pour encourager cet objectif, le protocole génère également un montant fixe de Pi qui sert de bonus de parrainage pour le parrain et le filleul (ou les deux parents et descendants :) Ce pool partagé peut être exploité par les deux parties au

cours de leur vie - lorsque les deux parties minent activement. Le parrain et le filleul peuvent tous deux puiser dans ce pool afin d'éviter les modèles d'exploitation où les filleuls sont en mesure de "s'attaquer" à leurs parrains. La prime de recommandation sert d'incitatif au niveau du réseau pour faire croître le réseau Pi tout en incitant les membres à s'engager activement à sécuriser le réseau.

D – Primes de récompense pour les développeurs (Pi supplémentaires frappés pour soutenir le développement en cours)
Pi financera son développement continu avec un "Developer Reward" qui est créé à côté de chaque pièce frappée pour le minage et des références. Traditionnellement, les protocoles de cryptomonnaies ont frappé une quantité fixe d'approvisionnement qui est immédiatement placée dans la trésorerie. Parce que l'offre totale de Pi dépend du nombre de membres du réseau, Pi prélève progressivement sa récompense de développeur au fur et à mesure que le réseau évolue. La frappe progressive de la récompense du développeur de Pi a pour but d'aligner les incitations des contributeurs de Pi avec la santé globale du réseau.

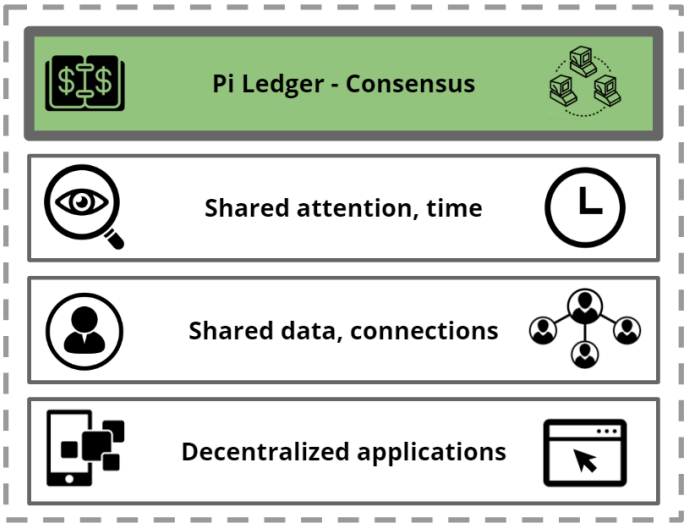
f est une fonction logarithmiquement décroissante - les premiers membres gagnent plus
Tandis que Pi cherche à éviter les concentrations extrêmes de richesse, le réseau cherche également à récompenser les membres antérieurs et leurs contributions par une part relativement plus importante de Pi. Lorsque des réseaux comme Pi en sont à leurs débuts, ils ont tendance à fournir une utilité moindre aux participants. Par exemple, imaginez avoir le tout premier téléphone au monde. Ce serait une grande innovation technologique, mais pas extrêmement utile. Cependant, à mesure que les gens acquièrent des téléphones, chaque titulaire de téléphone obtient plus d'utilité à partir du réseau. Afin de récompenser les personnes qui viennent au réseau plus tôt, la récompense minière individuelle de Pi et les récompenses de référence diminuent en fonction du nombre de personnes dans le réseau. En d'autres termes, il y a une certaine quantité de Pi qui est réservée pour chaque "slot" dans le réseau Pi.

Utilité : Mettre en commun et monétiser notre temps en ligne
Aujourd'hui, tout le monde est assis sur un véritable trésor de ressources inexploitées. Chacun d'entre nous passe des heures par jour sur son téléphone. Lorsque nous sommes au téléphone, chacun de nos points de vue, messages ou clics crée des profits extraordinaires pour les grandes entreprises. Chez Pi, nous croyons que les gens ont le droit de profiter de la valeur créée à partir de leurs ressources.

Nous savons tous que nous pouvons faire plus ensemble que seuls. Sur le web d'aujourd'hui, les grandes entreprises comme Google, Amazon, Facebook ont un effet de levier immense sur les consommateurs individuels. Par conséquent, ils sont en mesure de saisir la part de la valeur créée par les consommateurs individuels sur le Web. Pi égalise les règles du jeu en permettant à ses membres de mettre en commun leurs ressources collectives afin qu'ils puissent obtenir une part de la valeur qu'ils génèrent.

Le graphique ci-dessous est la pile Pi, où nous voyons des opportunités particulièrement prometteuses pour aider nos membres à capturer de la valeur. Ci-dessous, nous abordons chacun de ces domaines plus en détail.

Présentation de la pile de Pi : Libérer les ressources sous-utilisées



Pi Ledger (ç.à.d. Registre ou Grand livre de Pi) et graphique de confiance partagée

- Mise à l'échelle de la confiance sur le Web

L'un des plus grands défis sur Internet est de savoir à qui faire confiance. Aujourd'hui, nous nous appuyons sur les systèmes de notation de fournisseurs tels qu'Amazon, eBay, Yelp, pour savoir avec qui nous pouvons traiter sur Internet. Malgré le fait que nous, les clients, faisons le dur travail de notation et d'évaluation de nos pairs, ces intermédiaires Internet captent la part de la valeur créée par ce travail. L'algorithme de consensus de Pi, décrit ci-dessus, crée une couche de confiance native qui fait évoluer la confiance sur le web sans intermédiaires. Bien que la valeur du cercle de sécurité d'une seule personne soit minime, l'ensemble de nos cercles de sécurité individuels forment un " graphique de confiance " global qui aide les gens à comprendre qui, sur le réseau Pi, peut être fiable. Le graphique de confiance global du réseau Pi facilitera les transactions entre étrangers, ce qui n'aurait pas été possible autrement. La devise d'origine de Pi, à son tour, permet à tous ceux qui contribuent à la sécurité du réseau de capturer une part de la valeur qu'ils ont contribué à créer.

Pi's Attention Marketplace : Troc de l'attention et du temps inutilisés

Pi permet à ses membres de mettre en commun leur attention collective pour créer un marché de l'attention beaucoup plus précieux que l'attention d'un individu seul. La première application construite sur cette couche sera un canal de médias sociaux actuellement hébergé sur l'écran d'accueil de l'application. Vous pouvez considérer le rare canal de médias sociaux comme Instagram avec un message global à la fois. Les pionniers peuvent parier que Pi attirera l'attention des autres membres du réseau en partageant du contenu (p. ex. du texte, des images, des vidéos) ou en posant des questions qui visent à puiser dans la sagesse collective de la communauté. Sur le réseau Pi, tout le monde a la possibilité d'être un influenceur ou de puiser dans la sagesse de la foule. Jusqu'à présent, l'équipe centrale de Pi a utilisé ce canal pour sonder l'opinion de la communauté sur les choix de design pour Pi (par exemple, la communauté a voté sur le design et les couleurs du logo Pi.) Nous avons reçu de nombreuses réponses et commentaires précieux de la communauté sur ce projet. Une orientation future possible est d'ouvrir le marché de l'attention pour n'importe quel Pionnier d'utiliser Pi pour publier leur contenu, tout en augmentant le nombre de chaînes hébergées sur le réseau Pi.

En plus de troquer de l'attention avec leurs pairs, les pionniers peuvent également opter pour le troc avec des entreprises qui recherchent leur attention. L'Américain moyen voit entre 4 000 et 10 000 annonces par jour. Les entreprises se battent pour notre attention et paient d'énormes sommes d'argent pour cela. Mais nous, les clients, ne recevons aucune valeur de ces transactions. Dans le marché de l'attention de Pi, les entreprises cherchant à atteindre les Pionniers devront compenser leur audience en Pi. Le marché de la publicité de Pi sera strictement opt-in uniquement et donnera l'occasion aux Pionniers de monétiser l'une de leurs plus grandes ressources inexploitées : leur attention.

Pi's Barter Marketplace : Construisez votre vitrine virtuelle personnelle
En plus d'apporter confiance et attention au Réseau Pi, nous attendons des Pionniers qu'ils puissent apporter leurs compétences et services uniques dans le futur. L'application mobile de Pi servira également de point de vente où les membres de Pi pourront offrir leurs produits et services inexploités via une "vitrine virtuelle" aux autres membres du réseau Pi. Par exemple, un membre offre une chambre sous-utilisée dans son appartement à louer à d'autres membres du réseau Pi. En plus des atouts réels, les membres du réseau Pi pourront également offrir des compétences et des services via leurs vitrines virtuelles. Par exemple, un membre du réseau Pi pourrait offrir ses compétences en programmation ou en conception sur le marché Pi. Avec le temps, la valeur de Pi sera soutenue par un panier croissant de biens et services.

Pi's Decentralized App Store : Abaisser la barrière d'entrée pour les créateurs
La monnaie commune, le graphique de confiance et le marché du réseau Pi seront le terreau d'un écosystème plus large d'applications décentralisées. Aujourd'hui, quiconque veut démarrer une application doit redémarrer son infrastructure technique et sa communauté à partir de zéro. Le magasin d'applications décentralisées de Pi permettra aux développeurs Dapp de tirer parti de l'infrastructure existante de Pi ainsi que des ressources partagées de la communauté et des utilisateurs. Les entrepreneurs et les développeurs peuvent proposer de nouveaux Dapps (Applications Distribuées) à la communauté avec des demandes d'accès aux ressources partagées du réseau. Pi construira également ses Dapps avec un certain degré d'interopérabilité afin que les Dapps soient capables de référencer les données, les actifs et les processus dans d'autres applications décentralisées.

****

Gouvernance - Cryptomonnaie pour et par le peuple

Défis avec les modèles de gouvernance de 1ère génération
La confiance est le fondement de tout système monétaire réussi. L'un des facteurs les plus importants qui engendrent la confiance est la gouvernance, c'est-à-dire le processus par lequel des changements sont apportés au protocole au fil du temps. Malgré son importance, la gouvernance est souvent l'un des aspects les plus négligés des systèmes cryptoéconomiques.
Les réseaux de première génération tels que Bitcoin ont largement évité les mécanismes de gouvernance formels (ou "on-chain") au profit de mécanismes informels (ou "off-chain") issus d'une combinaison de conception des rôles et des incitations. Selon la plupart des mesures, les mécanismes de gouvernance de Bitcoin ont été très efficaces, ce qui a permis au protocole de prendre de l'ampleur

et de prendre de la valeur depuis sa création. Cependant, il y a aussi eu quelques défis. La concentration économique de Bitcoin a conduit à une concentration du pouvoir politique. Le résultat est que les gens ordinaires peuvent être pris au milieu de batailles destructrices entre les détenteurs massifs de Bitcoin. L'un des exemples les plus récents de ce défi est la bataille en cours entre Bitcoin et Bitcoin Cash. Ces guerres civiles peuvent se terminer dans un “Fork” où la Blockchain initiale donne lieu à deux Blockchains concurrentes. Pour les détenteurs de jetons, les Forks sont inflationnistes et peuvent menacer la valeur de leurs avoirs.

Le modèle de gouvernance de Pi : un plan en deux phases

Dans un article contestant les mérites de la gouvernance en chaîne, Vlad Zamfir, l'un des principaux développeurs d'Ethereum, affirme que la gouvernance en chaîne bloquée "n'est pas un problème de conception abstraite. C'est un problème social appliqué." L'un des points clés de Vlad est qu'il est très difficile de concevoir des systèmes de gouvernance " a priori " ou avant d'observer les défis particuliers posés par un système politique spécifique. La fondation des États-Unis en est un exemple historique. La première expérience de démocratie aux États-Unis, avec les articles de la Confédération, a échoué après une expérience de huit ans. Les Pères fondateurs des États-Unis ont alors pu tirer les leçons de l'article de la Confédération pour rédiger la Constitution - une expérience beaucoup plus réussie.

Pour bâtir un modèle de gouvernance durable, Pi poursuivra un plan en deux phases.

Modèle de gouvernance provisoire (< 5 millions de membres)

Jusqu'à ce que le réseau atteigne une masse critique de 5 millions de membres, Pi fonctionnera selon un modèle de gouvernance provisoire. Ce modèle ressemblera le plus aux modèles de gouvernance " hors chaîne " actuellement utilisés par des protocoles comme Bitcoin et Ethereum, l'équipe centrale de Pi jouant un rôle important dans l'élaboration du protocole. Cependant, l'équipe centrale de Pi continuera de dépendre fortement de l'apport de la communauté. L'application mobile Pi elle-même est l'endroit où l'équipe centrale de Pi a sollicité les commentaires de la communauté et s'est engagée auprès des Pionniers. Pi accepte les critiques et suggestions de la communauté, qui sont mises en œuvre par les fonctionnalités ouvertes aux commentaires de la page d'accueil de Pi, les FAQ et le livre blanc. Chaque fois que les gens parcourent ces documents sur les sites Web de Pi, ils peuvent soumettre des commentaires sur une section spécifique juste là pour poser des questions et faire des suggestions. Les rencontres hors ligne des pionniers organisées par l'équipe de base de Pi seront également un canal important pour l'apport de la communauté.

De plus, l'équipe centrale de Pi élaborera des mécanismes de gouvernance plus formels. Un système de gouvernance potentiel est la démocratie fluide. Dans une démocratie fluide, chaque pionnier aura la possibilité de voter directement sur une question ou de déléguer son vote à un autre membre du réseau. Une démocratie fluide permettrait à la communauté de Pi d'avoir des membres à la fois nombreux et efficaces.

La "Convention constitutionnelle" de Pi (> 5M membres)

Après avoir atteint 5 millions de membres, un comité provisoire sera formé sur la base des contributions précédentes au Réseau Pi. Ce comité sera chargé de solliciter et de proposer des suggestions de la part de l'ensemble de la communauté. Il organisera également une série de conversations en ligne et hors ligne où les membres de Pi pourront peser sur la constitution à long terme de Pi. Compte tenu de la base mondiale d'utilisateurs de Pi, le réseau Pi organisera ces conventions à plusieurs endroits à travers le monde pour assurer l'accessibilité. En plus d'organiser des conventions en personne, Pi utilisera également son application mobile comme plateforme pour permettre aux membres de Pi de participer au processus à distance. Que ce soit en personne ou en ligne,

les membres de la communauté Pi auront la possibilité de participer à l'élaboration de la structure de gouvernance à long terme de Pi.

****

FEUILLE DE ROUTE : Plan de déploiement

Phase 1 - Conception, distribution, Bootstrap du graphique de confiance.
Le serveur Pi fonctionne comme un robinet émulant le comportement du système décentralisé tel qu'il fonctionnera une fois qu'il sera opérationnel. Au cours de cette phase, il est possible et relativement facile d'améliorer l'expérience et le comportement de l'utilisateur par rapport à la phase stable du réseau principal. Toutes les pièces frappées par les utilisateurs seront migrées vers le réseau vivant une fois qu'il sera lancé. En d'autres termes, le livenet pré-monnaie dans sa genèse bloquera tous les soldes des titulaires de comptes générés au cours de la phase 1, et continuera à fonctionner comme le système actuel mais entièrement décentralisé. Pi n'est pas coté en bourse pendant cette phase et il est impossible d'"acheter" Pi avec une autre devise.

Phase 2 - Testnet
Avant de lancer le réseau principal, le logiciel Node sera déployé sur un réseau de test. Le réseau de test utilisera le même graphique de confiance que le réseau principal mais sur une pièce de monnaie Pi de test. Pi accueillera plusieurs nœuds sur le réseau de test, mais encouragera plus de Pionniers à créer leurs propres nœuds sur le réseau de test. En fait, pour qu'un nœud puisse rejoindre le réseau principal, il est conseillé de commencer sur le testnet. Le réseau de test sera exécuté en parallèle de l'émulateur Pi dans la première phase, et périodiquement, par exemple quotidiennement, les résultats des deux systèmes seront comparés pour détecter les lacunes et les manques du réseau de test, ce qui permettra aux développeurs Pi de proposer et de mettre en œuvre des corrections. Après une exécution simultanée complète des deux systèmes, testnet atteindra un état où ses résultats correspondront systématiquement à ceux de l'émulateur. Lorsque la communauté se sentira prête, Pi passera à la phase suivante.

Phase 3 - Mainnet
Quand la communauté sentira que le logiciel est prêt pour la production et qu'il aura été testé à fond sur le testnet, le réseau principal officiel du réseau Pi sera lancé. Un détail important est que, lors de la transition vers le réseau principal, seuls les comptes validés pour appartenir à des individus réels distincts seront honorés. Après ce point, le robinet et l'émulateur réseau Pi de la phase 1 seront arrêtés et le système continuera tout seul pour toujours. Les futures mises à jour du protocole seront apportées par la communauté des développeurs Pi et l'équipe centrale de Pi, et seront proposées par le comité. Leur mise en œuvre et leur déploiement dépendront de la mise à jour du logiciel de minage par les nœuds, comme n'importe quelle autre chaîne de blocs. Aucune autorité centrale ne contrôlera la monnaie et celle-ci sera entièrement décentralisée. Les soldes des faux utilisateurs ou des utilisateurs dupliqués seront jetés. C'est la phase où Pi peut être connecté aux échanges et être échangé contre d'autres devises.