Bitnet: Un réseau monétaire programmable de pair à pair

Masayoshi Kobayashi
masayoshikob@gmail.com
www.bitnet.money

Résumé. Les réseaux pair à pair basés sur la technologie blockchain ont rendu possible le transfert de valeur d'un individu à un autre sans avoir besoin d'une institution financière intermédiaire, permettant ainsi la garde autonome et le contrôle total des fonds par les participants individuels de ces réseaux. L'évolution de la technologie a commencé avec le lancement de Bitcoin en 2009, avec une avancée supplémentaire réalisée par Ethereum en 2015 avec l'introduction de contrats intelligents, rendant l'argent hautement programmable, permettant la tokenisation de la valeur à travers des actifs fongibles et non fongibles, et plus encore. L'objectif initial de Bitcoin était de servir de moyen d'échange décentralisé, mais pour des raisons que nous expliquerons plus en détail dans cet article, il a échoué dans sa mission principale et s'est plutôt transformé en ce qui pourrait être comparé à une version numérique de l'or ou à une réserve de valeur décentralisée. Ethereum, quant à lui, permet la mise en œuvre d'une technologie de paiement plus adéquate mais ne parvient pas à être suffisamment décentralisé, avec plus de la moitié de son offre actuelle en circulation (environ 70 millions sur 120 millions, au moment de la rédaction) étant pré-minée, créant ainsi une répartition inégale et injuste de l'offre en circulation d'ETH, ce qui s'ajoute au fait qu'il est passé d'un mécanisme de consensus efficace et véritablement décentralisé, PoW, à un mécanisme de consensus PoS non éprouvé et quelque peu fragile, favorisant davantage les gros détenteurs au détriment des nouveaux venus. Il a également un PDG désigné et une équipe de développement centralisée et concentrée, qui détiennent de facto le pouvoir de décider de la mise en œuvre de propositions d'amélioration qui pourraient influencer le prix, l'adoption et la distribution de l'ETH, faisant de cette monnaie plus semblable à un titre qu'à un moyen d'échange réellement décentralisé. Bitnet vise à résoudre ces problèmes en concevant une implémentation PoW d'Ethereum qui fonctionne en parallèle avec Bitcoin et sert de véhicule véritablement décentralisé pour l'argent programmable, avec une politique monétaire intégrée qui favorise son utilisation comme moyen d'échange plutôt que comme réserve de valeur, avec un mécanisme de création d'offre prévisible et codifié qui permet une croissance saine de l'offre dans le temps pour favoriser l'expansion économique, la véritable décentralisation et l'équité.

1. Introduction

La conception de ce qui est maintenant connu sous le nom de technologie de la blockchain par Satoshi Nakamoto en 2009 avec la création de Bitcoin a été un pilier pour le développement de technologies décentralisées qui facilitent les paiements à travers le monde et permettent aux individus de prendre le contrôle de leurs finances grâce à l'autodétention. Cela a marqué un changement générationnel dans notre compréhension et notre utilisation de l'argent. Cette tendance a été encore exacerbée par le lancement d'Ethereum en 2015 et l'introduction des contrats intelligents, qui ont essentiellement permis à l'argent d'être programmable et de répondre aux différents besoins financiers de différentes niches de la société, tout en facilitant une nouvelle ère du commerce numérique avec la preuve de propriété de jetons non fongibles, à la fois entièrement numériques et en représentation d'actifs non fongibles du monde réel.

Cependant, à la fois Bitcoin et Ethereum présentent des défauts de conception ou de conception qui les rendent inadaptés à une utilisation conforme à leur intention initiale, dans le cas de Bitcoin, ou fragiles et susceptibles de défaillance en raison de la centralisation, dans le cas d'Ethereum.

Bitnet vise à résoudre ces problèmes en concevant une implémentation de Preuve de Travail d'Ethereum qui fonctionne en parallèle avec Bitcoin et sert la société en tant que véhicule véritablement décentralisé pour l'argent programmable, avec une politique monétaire intégrée qui favorise son utilisation comme moyen d'échange plutôt que comme réserve de valeur, avec un mécanisme de création de l'offre prévisible et codé en dur qui permet une croissance saine de l'offre au fil du temps pour favoriser l'expansion économique, la décentralisation véritable et l'équité pour les nouveaux utilisateurs.

2. Le problème du Bitcoin

Le Bitcoin a été créé pour fonctionner comme un système de paiement électronique de pair à pair, mais malgré ses qualités intrinsèques, il échoue à le faire par conception, en raison de sa politique monétaire déflationniste, de son offre limitée et de son manque de programmabilité. Ces contraintes réduisent ses cas d'utilisation tout en entravant son utilisation en tant que monnaie en raison des longs délais de règlement, des problèmes de scalabilité et des transactions coûteuses.

a. **Une politique monétaire déflationniste entraîne une sur spéculation et d'autres problèmes**

Le Bitcoin est programmé pour avoir seulement 21 000 000 de BTC en circulation, ce qui va à l'encontre de l'idée qu'il puisse être utilisé comme monnaie en raison de ses propriétés déflationnistes inhérentes. Les détenteurs sont dissuadés de dépenser leurs Bitcoins car ils savent que plus le protocole se développe et plus de personnes l'utilisent, la demande accrue à elle seule fera monter son prix, le rendant toujours plus précieux à l'avenir qu'il ne l'est maintenant. Une monnaie est censée être utilisée comme moyen d'échange de valeur entre individus dans les transactions quotidiennes. En rendant une monnaie déflationniste par conception, les créateurs de cette monnaie entravent implicitement l'expansion économique et son utilisation par les détenteurs en tant que monnaie réelle, car ils auront tendance à toujours spéculer ou seront moins enclins à dépenser afin de profiter de l'appréciation future probable de leurs avoirs, et cela peut entraîner ce qu'on appelle une spirale déflationniste, aboutissant à une récession ou une dépression économique. La politique monétaire intégrée dans le Bitcoin en fait une excellente réserve de valeur numérique, mais pas tellement une monnaie.

b. **L'offre limitée peut conduire à des rachats par de grandes institutions ou des individus avant que l'adoption de masse réelle ne se produise**

Au moment de la rédaction de cet article, la capitalisation boursière du Bitcoin se situe autour de 590 milliards de dollars américains. Pour comparaison, la capitalisation boursière de l'or est actuellement d'environ 12,8 billions de dollars américains. À l'heure actuelle, environ 19,4 des 21 millions de Bitcoins existants ont déjà été minés. Cela illustre à quel point le Bitcoin est petit par rapport à d'autres actifs comparables, et cela crée un problème car il favorise l'inégalité en permettant aux grandes institutions d'acheter des sommes disproportionnées de l'offre totale du marché du Bitcoin, en rompant avec l'éthique de sa propre création en favorisant de manière disproportionnée ceux que le Bitcoin visait à perturber. Nous voyons cela se produire chaque jour avec de plus en plus d'entreprises cotées en bourse détenant du Bitcoin dans leurs bilans d'entreprise, et même certaines banques centrales du monde commencent à le faire. Cela entraîne une concentration excessive de l'offre et retire le pouvoir à l'individu pour le transférer tacitement à ceux qui en ont le moins besoin

c. **Le Bitcoin n'est pas programmable, ce qui crée une autre couche de problèmes pour son adoption en tant que monnaie plutôt qu'en tant que réserve de valeur**

Différentes nations et sociétés ont des besoins financiers différents, et souvent une approche "taille unique" en matière de politique monétaire créera très probablement des disparités entre différentes couches de la société et favorisera ou nuira de manière disproportionnée aux individus en fonction de leurs circonstances personnelles. La monnaie numérique doit être programmable, afin de pouvoir répondre et s'adapter aux différents besoins des différentes nations, communautés, entreprises et individus. Elle doit être décentralisée dans son essence tout en permettant à l'argent privé d'exister également en parallèle

3. Le problème d'Ethereum

Ethereum est venu résoudre de nombreux problèmes que Bitcoin a en tant que monnaie, mais il n'a pas réussi à atteindre une véritable décentralisation et, après être passé d'un mécanisme de consensus de preuve de travail à preuve d'enjeu, il s'est rendu encore plus fragile et vulnérable aux actions d'application de la loi par les régulateurs qui ne devraient pas avoir leur mot à dire dans le fonctionnement des protocoles décentralisés.

a. **Ethereum a connu un lancement injuste, avec près de 60 % de l'offre totale en circulation, au moment de la rédaction de cet article, étant pré-minée et distribuée parmi les premiers investisseurs et les fondateurs**

Contrairement au Bitcoin, environ 70 millions des quelque 120 millions de jetons ETH en circulation aujourd'hui ont été pré-minés et distribués aux premiers investisseurs et fondateurs. Bien que la prémisse de récompenser les premiers adoptants soit valable en raison de la matrice de risque qu'elle présente, le lancement d'Ethereum était loin d'être équitable et, dès le premier jour, il a créé des gagnants et des perdants dans le protocole et a laissé une tâche permanente qui ne sera jamais oubliée.

b. **La preuve d'enjeu est un système novateur, fragile et non éprouvé, et favorise l'inégalité par conception**

Le concept de preuve de travail remonte à 1993, lorsque Cynthia Dwork et Moni Naor cherchaient une solution pour dissuader le spam par e-mail et les attaques par déni de service, et depuis lors, il a été utilisé dans de nombreuses applications à grande échelle, ce qui en fait un mécanisme robuste et bien éprouvé pour sécuriser un réseau blockchain. En résumé, dans le contexte d'une blockchain, la preuve de travail implique que des ordinateurs résolvent des problèmes mathématiques complexes pour valider et soumettre de nouveaux blocs au réseau. La preuve d'enjeu, en revanche, a été récemment conçue dans le but de contourner les problèmes de scalabilité de Bitcoin, mais elle favorise la centralisation du capital et favorise les gros

détenteurs, qui peuvent déposer leurs jetons dans le protocole pour recevoir des récompenses de blocs, sans travail, sans entretien ni échange. Cela fonctionne un peu comme un compte d'épargne perpétuel, où les gros détenteurs collectent des récompenses de blocs et des frais auprès des utilisateurs moins favorisés sans rien donner en retour au réseau, si ce n'est leur promesse de ne rien faire de mauvais ou de malhonnête. La preuve de travail récompense un travail réel et un échange tangible entre les mineurs et le protocole, où les mineurs échangent de la puissance de calcul et de l'énergie contre de la monnaie. La preuve d'enjeu apporte un ensemble d'autres problèmes - tels que la susceptibilité aux actions d'application de la loi par les régulateurs - qui sortent du cadre de cet article, mais les lecteurs sont incités à se renseigner sur les risques potentiels associés à l'utilisation de la preuve d'enjeu pour sécuriser ce qui devrait être un protocole décentralisé. Une monnaie vraiment mondiale et décentralisée ne peut pas utiliser un mécanisme de consensus qui favorise les gros investisseurs et les institutions au détriment des utilisateurs particuliers. En faisant cela, un tel protocole fait partie du système financier mondial existant, et non une alternative à celui-ci.

c. Ethereum possède une équipe centrale de développement très centralisée et un PDG

Ethereum et ETH ont plus en commun avec les sociétés privées et les titres financiers qu'avec une monnaie véritablement décentralisée. Avoir un PDG, des développeurs qui détiennent le pouvoir de facto sur les modifications apportées au protocole, et une fondation qui échange ses propres jetons natifs ne ressemble pas à une technologie qui peut être appliquée sans crainte pour créer le nouveau système financier mondial. Une preuve du niveau d'autorité que les développeurs ont sur le protocole est le “fork” de la DAO qui s'est produit en 2016, lorsqu'ils ont choisi de revenir en arrière sur ce qui aurait dû être des transactions immuables pour contourner une tentative de piratage réussie dans l'un de ses protocoles "décentralisés" les plus importants à l'époque, forçant indirectement les mineurs à suivre la nouvelle chaîne et à l'adopter comme le véritable réseau Ethereum, ou à l'abandonner et à risquer de perdre tous leurs revenus. Et pour ceux qui feraient valoir qu'Ethereum Classic serait une bonne alternative, il partage toujours une histoire commune avec Ethereum jusqu'à ce bloc du “fork”, partageant ainsi tous les mêmes défauts fondamentaux qui rendent Ethereum lui-même inadapté à être utilisé comme un réseau d'argent programmable entièrement décentralisé, y compris l'offre pré-minée. Tout comme tous ses concurrents de contrats intelligents, Ethereum a été fondé sur un terrain inadapté, et il n'y a pas de retour en arrière possible.

4. Bitnet

Le monde n'a pas encore vu de réseau d'argent programmable véritablement décentralisé, sans aucun contrôle central, impartial et construit sur des bases solides, permettant son utilisation en tant que réseau de paiement mondial sans les risques associés à Ethereum et aux autres réseaux centralisés de contrats intelligents basés sur la blockchain. Pour y parvenir, un tel protocole doit être conçu selon les principes fondamentaux suivants:

- Ne pas avoir d'approvisionnement pré-miné ou d'allocations privées, y compris celles de l'équipe de développement
- Être gratuit pour que tout le monde puisse participer, ne pas avoir de PDG et être capable de favoriser une communauté centrale qui apprécie les valeurs de la décentralisation et de l'équité pour le nouveau système financier mondial
- Être programmable afin de pouvoir s'adapter et répondre aux différents segments de la société avec différentes formes de monnaie, y compris la monnaie privée
- Avoir un approvisionnement inflationniste prévisible pour éviter les prises de contrôle à long terme et permettre une expansion économique
- Utiliser un mécanisme de consensus de preuve de travail qui impliquera l'échange tangible d'énergie et de puissance de calcul pour la création de nouveaux approvisionnements

a. Infrastructure technologique

Comme Bitcoin présente des contraintes technologiques intrinsèques qui en font une excellente réserve de valeur tout en en faisant une forme de monnaie inadéquate, les principales contraintes et problèmes d'Ethereum sont conceptuels et fondamentaux, ce qui en fait une excellente base pour le lancement de Bitnet. Le code d'Ethereum est open-source et a été largement testé depuis sa création en 2015. Il sera utilisé pour la mise en œuvre initiale du client central Bitnet. Le réseau fonctionnera sur un mécanisme de consensus de preuve de travail et récompensera les mineurs pour leur travail en créant de nouveaux approvisionnements, favorisant ainsi un taux d'inflation prévisible qui permet une expansion économique et une demande accrue à mesure que le protocole se développe. La vitesse à laquelle le code central serait mis à jour serait beaucoup plus lente que celle des protocoles centralisés existants ; tout comme l'or n'a pas changé au cours des mille dernières années, une forme véritablement efficace de monnaie devrait être conçue avec des propriétés d'une qualité suffisante pour que les mises à jour et les changements puissent être minimes. Les modifications apportées au code central devraient être proposées conformément aux principes de décentralisation et ne seraient mises en œuvre qu'après un consensus clair entre les mineurs et les utilisateurs du réseau.

b. Politique monétaire

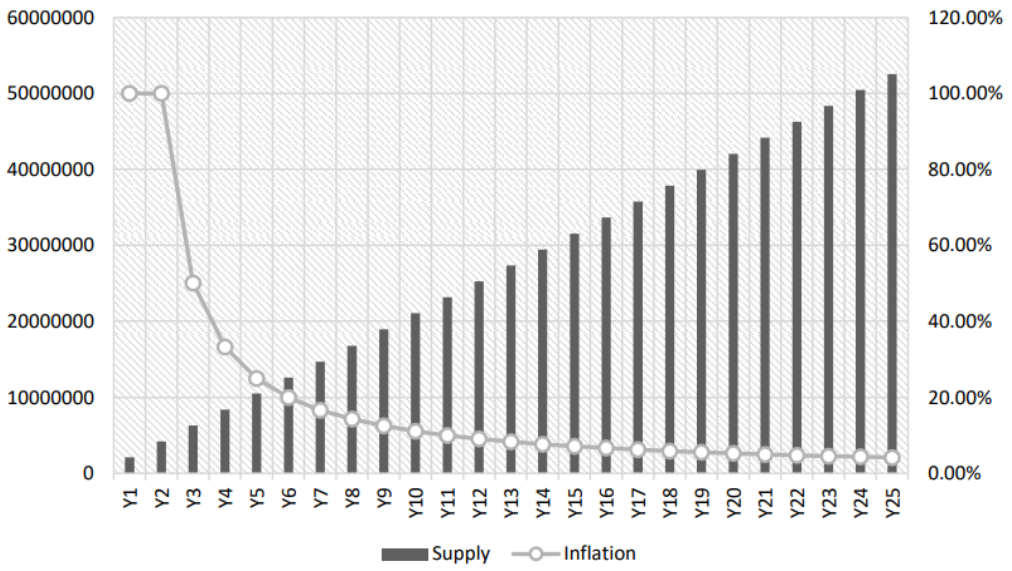
La politique monétaire du protocole sera codée en dur et prévoira un approvisionnement inflationniste à un rythme prévisible, où un nouvel approvisionnement est créé lors de la soumission réussie d'un nouveau bloc au réseau, puis récompensé au mineur.

1. Temps de bloc et taux d'inflation

Le réseau a une moyenne de 15 secondes entre les blocs par conception, et lors de la réussite de l'extraction d'un nouveau bloc, 1 nouveau Bitnet est créé. Comme les temps de bloc peuvent varier en raison de la nature de la preuve de travail, ce schéma crée une constante semi-constante de 2 102 400 nouveaux Bitnets ajoutés à l'approvisionnement mondial chaque année:

*4 blocs par minute * 60 minutes * 24 heures * 365 jours = 2,102,400*

Cela crée une dynamique où le taux d'inflation diminue à mesure que plus de blocs sont ajoutés au réseau - car le nouvel approvisionnement sera toujours ajouté au-dessus de l'approvisionnement existant précédemment, mais n'atteindra jamais zéro.
Le taux d'inflation dynamique avec un taux de récompense fixe permet une inflation plus agressive au cours des premières années du protocole, ce qui contribuera à promouvoir la croissance économique et l'adoption, et à mesure que le protocole mûrit et que le taux d'inflation diminue, la thèse est qu'il y aurait moins de volatilité sur le marché et plus de cohérence des prix, renforçant ainsi le rôle de Bitnet en tant que forme de monnaie décentralisée.
Le graphique ci-dessous illustre le taux d'inflation attendu pour les 25 premières années du protocole par rapport à la création d'approvisionnement pour la même période. Une remarque importante est que les premières années d'inflation présentent des taux plus élevés en raison de l'inexistence d'un approvisionnement initial auquel se référer - car si nous ajoutons 1 unité à 1 unité, nous avons une augmentation de 100 %, si nous ajoutons 1 unité à 100 unités, nous n'aurions qu'une augmentation de 1 %, même si en termes absolus, le taux d'inflation serait toujours le même.



Le tableau ci-dessous illustre le taux d'inflation prévu pour les 50 premières années d'existence du protocole.

Year 1	100%	Year 11	10%	Year 21	5%	Year 31	3.33%	Year 41	2.5%
Year 2	100%	Year 12	9.09%	Year 22	4.76%	Year 32	3.23%	Year 42	2.44%
Year 3	50%	Year 13	8.33%	Year 23	4.55%	Year 33	3.13%	Year 43	2.38%
Year 4	33.33%	Year 14	7.69%	Year 24	4.35%	Year 34	3.03%	Year 44	2.33%
Year 5	25%	Year 15	7.14%	Year 25	4.17%	Year 35	2.94%	Year 45	2.27%
Year 6	20%	Year 16	6.67%	Year 26	4%	Year 36	2.86%	Year 46	2.22%
Year 7	16.67%	Year 17	6.25%	Year 27	3.85%	Year 37	2.78%	Year 47	2.17%
Year 8	14.29%	Year 18	5.88%	Year 28	3.7%	Year 38	2.7%	Year 48	2.13%
Year 9	12.5%	Year 19	5.56%	Year 29	3.57%	Year 39	2.63%	Year 49	2.08%
Year 10	11.11%	Year 20	5.26%	Year 30	3.45%	Year 40	2.56%	Year 50	2.04%

2. Récompenses et frais

Les mineurs seront incités à participer et à sécuriser le protocole en recevant une nouvelle offre et des frais d'utilisation pour chaque bloc miné. Pour chaque transaction soumise au réseau, les utilisateurs devront payer des frais, appelés gaz. Les frais de gaz sont mesurés en Gwei, et chaque Gwei équivaut à 1e-9 de Bitnet. Le montant que les utilisateurs paieront en frais de gaz est dynamique et reflète la capacité d'utilisation du réseau à un moment donné.

c. Performance attendue

Bitnet aura la fiabilité et la décentralisation à son cœur et sera conçu pour servir de base pour d'autres innovations et solutions de mise à l'échelle de la couche 2 potentielles qui peuvent ajouter à la performance globale du réseau et aux cas d'utilisation. Pour augmenter le débit, Bitnet permet des tailles de bloc jusqu'à 10 fois plus grandes que celles d'Ethereum, capable de traiter jusqu'à 7 142 transactions brutes par bloc, soit 476 transactions brutes par seconde. La capacité supplémentaire ne signifie pas nécessairement que les transactions seront traitées plus rapidement que sur Ethereum, mais que le réseau dispose d'une plus grande capacité pour traiter plusieurs transactions simultanément.

5. L’objectif

L’objectif principal de l'existence de Bitnet est d'être une technologie de base décentralisée qui peut être utilisée par des particuliers, des entreprises et des gouvernements pour façonner le nouveau système financier mondial; un système qui est inclusif, autonome, décentralisé, international et surtout, qui donne le pouvoir à l'individu de choisir comment gérer son propre argent, sans les contraintes de dépendre de services de garde centralisés, d'entreprises ou de gouvernements.

6. Conclusion

À ce jour, le marché des actifs numériques n'a qu'un seul protocole véritablement décentralisé, qui est le Bitcoin. Cependant, Bitcoin présente des défauts de conception fondamentaux qui l'empêchent de devenir une monnaie mondiale, et la preuve en est que la perception de Bitcoin tend de plus en plus vers une réserve de valeur plutôt que de l'argent, étant souvent appelé or numérique. Ethereum, qui est de loin le protocole le plus important ayant la technologie capable de permettre ce qui pourrait être de l'argent programmable à l'échelle mondiale, manque de décentralisation et de distribution équitable des fonds pour le faire. Bitnet fusionne les qualités inhérentes qui font de Bitcoin une solide réserve de valeur décentralisée et la technologie d'Ethereum pour créer ce qui est une véritable monnaie mondiale pouvant être utilisée par n'importe qui, n'importe où, et qui ne peut pas être fermée ou réglementée. Il permet également la création d'argent programmable privé ou souverain, la tokenisation de la valeur sur internet, l'émission de jetons non fongibles et la mise en œuvre de solutions de mise à l'échelle qui tireraient parti de la décentralisation et de la sécurité de Bitnet pour créer des solutions de niveau 2 spécialement conçues.