Woodcoin: Une monaie Peer to peer électronique construite pour la longévité et stable.

Funkenstein le Nain
Le 31 octobre 2014

Abstrait:

Nous décrivons ici les considérations relatives à la conception et la mise en œuvre des bois, en Qui le séparent des autres cryptocurrencies. Woodcoin est une cryptocourance très semblable Bitcoin. Cependant, la conception de bitcoin modélise explicitement une ressource non renouvelable: l'or. Pour Woodcoin nous modelons plus étroitement une ressource durable. En particulier, le boeuf évite le temps Asymétries du modèle de libération de bitcoin, maximisant l'incitation à participer et la longévité De la pièce de monnaie en même temps. Notre solution est la croissance logarithmique de la masse monétaire. En outre, Nous décrivons les considérations de conception derrière deux autres changements au protocole de base: l'extraction avec le Fonction de hachage Skein et sécurisation de la propriété numérique avec la courbe X9_prime256v1 en utilisant ECDSA.

Introduction:

Il y a six ans, le grand sorcier Satoshi Nakamoto a livré la terre moyenne aux griffes des Contrefaçons en publiant l'algorithme de preuve de travail lors de la première mise en œuvre d'un Cryptocourance: bitcoin [Nakamoto, 2008]. Notre travail actuel, le bois, est un Cryptocurrency qui est construit de la même façon que bitcoin, le partage dans la base de code avec Bitcoin et deux de ses successeurs: litecoin et quark. L'objectif du boisé est de prendre un À long terme et de concevoir une pièce qui reste viable et stable très loin dans l'avenir.

$$R_n = K / 2 ^ n \qquad (1)$$

Ici , R n est la récompense à un pas de temps n, et k est une constante initiale (k = 50 pour bitcoin classique)

Ceci est connu mathématiquement en langue commune comme une série géométrique, dont la somme converge rapidement avec l' augmentation n. Le résultat est qu'après les quatre premières années, la moitié de la CTB Out avait

été libéré. En outre, il y aura un moment relativement proche où la récompense Bloc approche zéro, et d'autres activités minières devront être encouragées par les frais de transaction seuls. Il N'est pas clair comment bitcoin et autres cryptocurrencies se comporteront dans cette limite. Le problème est que le Coût de l'exécution d'un seul bloc double dépenser est proportionnelle à la récompense minière.
Ce sont ces propriétés que nous souhaitons améliorer avec une pièce de libération logarithmique. Pour les bois, nous Adoptent au lieu d'une série géométrique un harmonique, dans lequel la récompense est donnée par:

$$R\_n = K / N \qquad (2)$$

Dans ce cas il y a une différence immédiate qui est que la somme de la série ne converge pas. En théorie, cela signifierait une offre monétaire infinie, mais parce que nous sommes limités à la la plus petite récompense possible à 1 satoshi (10 -8 LOG), il y aura également une limite finale.

Cependant, la série harmonique croît incroyablement lentement. Le temps de la récompense finale arrivera lorsque R n = 10 -8 . Pour woodcoin nous avons choisi k = 1000000 et nous avons donc voir le LOG finale satoshi libéré au bloc n = 10 14 , Quelque part près de ce que les hommes appelleront année julienne 380 millions. Ce maximum de la masse monétaire qui sera atteint cette année est un peu plus de 27.625.814 LOG.

Alors que Bitcoin a publié la moitié de la CTB en quatre ans, nous prévoyons que la moitié du LOG sera publiée Quelque part dans l'année Julian 2305. L'offre totale d'argent de LOG à une hauteur de bloc n est déterminée en additionnant toutes les récompenses Pour les blocs précédents:

$$S\ n = \Sigma(i=100 \rightarrow n)\ \ K / i \approx k \cdot \log (n + \gamma) - F \qquad (3)$$

Où l'approximation est due au grand magicien Euler. Ici, γ est l'Euler-Mascheroni constant ~ 0,577, et le journal est le logarithme naturel. F représente la taille de la forêt, qui se compose De ces blocs initiaux pour lesquels le bois non ajouté à la fourniture:

$$F = \Sigma\ (N=0->100)\ k / N = 5\ 187\ 377 \qquad (4)$$

La forêt est introduite pour éliminer la récompense extrêmement élevée des premiers blocs et pour Rationnelle d'une ressource renouvelable.
Certaines cryptomonnaies ont choisi d'introduire à un moment donné une récompense constante fixe (par exemple Dogecoin). Cela impliquera éventuellement une inflation linéaire et une dépréciation de la monnaie existante, Éviter cette approche. D'autres pièces ont introduit une récompense proportionnelle à certaines externalités telles que Le hashrate (par exemple peercoin). Nous rejetons également cette approche en raison de l'incertitude Les calculs de la masse monétaire et le potentiel d'inflation future linéaire. Ces approches Tenter d'accroître la longévité des pièces en assurant un intérêt à l'extraction de la pièce, mais à un coût. Avec le Bois, nous assurons la longévité d'une incitation à la coupe du bois, mais sans le négatif Effets d'une inflation illimitée ou incertaine.
La courbe de libération lisse du bois est peut-être mieux illustrée en traçant la masse monétaire totale Par rapport au nombre de blocs, que nous montrons aux figures 1 et 2.

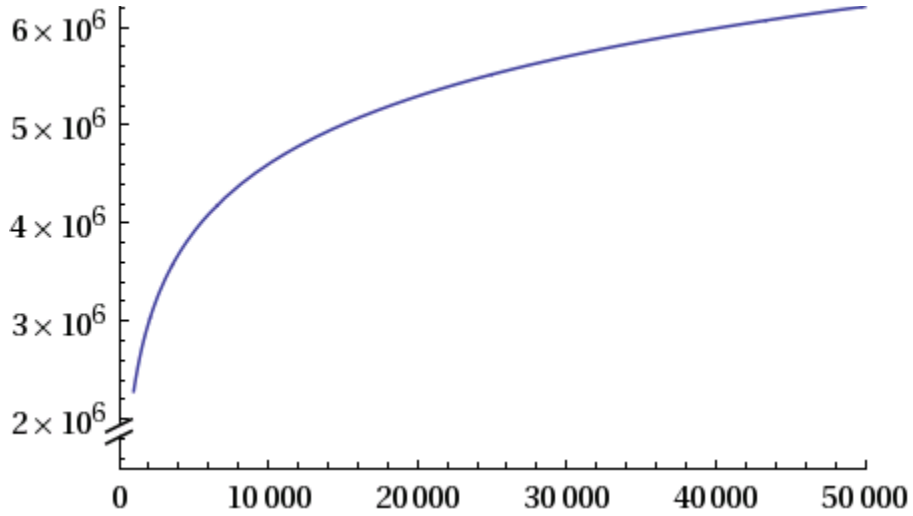

Figure 1 Approvisionnement total en bois pour les blocs 0 à 50000.

Comme on peut le constater en comparant les Figures un et deux, une caractéristique importante de la fonction logarithmique Est la similarité de soi. À chaque bloc, la récompense continue à baisser et un bûcheron Avantage sur tout futur bûcheron. L'incitation à couper le bois dans le moment présent Reste et n'est pas artificiellement diminuée.

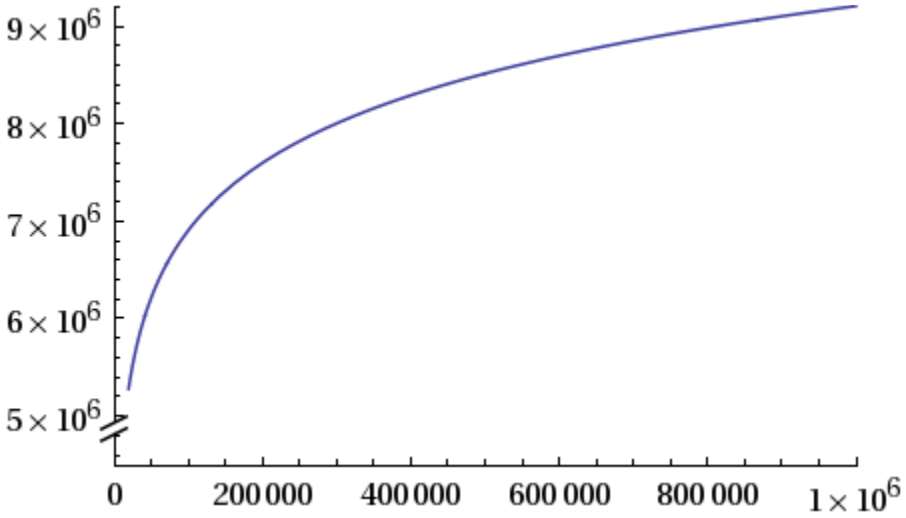

Figure 2. Approvisionnement total en bois pour les blocs 0 à 1 million

Algorithme de preuve de travail En choisissant une fonction de hachage pour laquelle fournir une preuve de travail et des blocs de formulaire qui vérifient Transactions, il ya beaucoup de diversité dans le monde cryptocurrency. De nombreuses pièces choisissent des fonctions Qui tentent de permettre à des CPU ordinaires de mener sans inciter au matériel spécialisé. Si ces pièces réussissent à gagner de la valeur, elles échoueront dans cet effort, comme tous les algorithmes

pourraient être Plus rapide sur le bon matériel. Pour notre choix de la fonction de hachage nous n'essayons pas d'éviter ASIC ou GPU, mais nous choisissons plutôt une fonction de hachage que nous trouvons la plus sûre Et compris dans ses mises en œuvre. La description et la promotion de la fonction Skein est la meilleure Laissé à ses créateurs [Ferguson et al., 2008], et dépasse le cadre de cet article. Cependant, nous Deux faits sur le Skein a fonction ici:

1) Il a été créé en partie par Bruce Schneier
2) La NSA n'a pas été choisie comme étant la fonction de hachage SHA3 officielle.

Choix de courbe elliptique pour ECDSA

Peut-être la technologie la plus importante qui rend une cryptocourance possible est une signature numérique Algorithme qui permet à un participant de prouver la propriété d'une pièce de monnaie, et donc de la dépenser. Ce La technologie a été popularisée en 1976 par les grands sorciers Whitfield Diffie et Martin Hellman. Une discussion approfondie de l'histoire échappe au cadre de cet article, mais il convient de noter que leur Le document de 1976 prévoyait déjà la montée des produits de l'échange numérique. Comme la plupart des cryptocurrences, Nous choisissons d'utiliser un algorithme différent de celui introduit dans ce document pour former des données numériques Signatures: nous utilisons l'Algorithme de signature numérique de courbe elliptique (ECDSA). Utilisation de ce système Nécessite le choix d'une courbe elliptique particulière. Une fois la courbe choisie, une clé privée peut être Choisie en sélectionnant un point sur cette courbe. Bien que nous ne connaissions aucune faiblesse Choix de courbes populaires, nous profitons de l'occasion pour introduire une nouvelle diversité cryptographique et Choisir une courbe différente que la plupart des autres cryptocurrencies, qui utilisent une courbe connue sous le nom secp256k1. La courbe que nous utilisons est connue sous le nom ANSI X9.62 Prime 256v1 et elle a été publiée comme recommandée Pour les institutions financières avant le tournant du siècle [ANSI,

1999]

Conclusions:

En lisant la discussion technique ci-dessus sur les propriétés de la woodcoin, un élément important a Été laissé de côté. Nous avons raté la forêt en regardant les arbres. La coupe du bois est un Une nouvelle façon d'aborder la cryptocourance et de nous encourager à quitter les mines pour un Émerveillez-vous de la beauté du bois. Découper le bois est exaltant, et pendant que nous woodcut nous pouvons penser De cette ressource se poursuit dans le futur en raison de notre planification minutieuse et durable. Nous avons aussi Souvenir de l'importance de maintenir une forêt, un écosystème diversifié, et de considérer et de L'intelligence des arbres et le don de l'air frais frais. À mesure que les cryptocou- Les sources d'énergie non renouvelables deviennent encore plus épuisées, on s'attend à ce que la double utilisation du hachage Les grumes et le chauffage des maisons deviendront plus répandus. Le bois est une ressource importante dans d'autres Compétences, ainsi, et nous espérons développer LOG pour être utilisé pour une variété de cryptocurrency autre Applications dès que des transactions de chaîne croisée atomique sont implémentées.

"Les chaînes de blocs sont des bases de données structurées en log" - Funkenstein the Dwarf

Les références:

1) "Bitcoin: une monnaie électronique pair à pair", Satoshi Nakamoto, 31 octobre 2008
2) «La famille de la fonction Hash de Skein», Niels Furguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, Jesse Walker, 15 novembre 2008
3) ANSI X9.62, «Cryptographie à clé publique pour l'industrie des services financiers: la courbe elliptique Algorithme de signature numérique (ECDSA) », 1999