La BlockChain expliqué

1. Code de la blockchain

le code qui va gérer une transaction entre deux pair va générer un horodatage pour pouvoir dater les transactions, une variable pour la preuve de travail sera créée et implémentée a chaque nouveau bloc créé, un hash sera stock dans chaque block ainsi que un hash precedent qui sera lié derriere chaque nouveau bloc.

1. Réseau

les pairs peuvent être sépare en deux groupes ceux qui sont sont en ecoute sur les connexions entrantes sur les port reservés a la blockchain et ceux qui y sont fermé, c'est-à-dire les pairs derrière un NAT a cause de l’absence de la route, ou bien a cause d’un pare-feu qui bloque le port de service. Les utilisateurs Bitcoin qui se connectent au réseau Bitcoin via Tor ou via un VPN n’acceptent évidemment pas non plus les connexions entrantes.

1. Protection anti-dos Bitcoin

La blockchain implémentent un protocole basé sur la réputation, chaque nœud conservant un score de pénalité pour chaque autre homologue Bitcoin (identifié par son adresse IP). Chaque fois qu'un message mal formé est envoyé au nœud, ce dernier augmente le score de pénalité (différents messages encourent des pénalités différentes) de l'expéditeur et bannit l'adresse IP « qui se comporte mal » pendant 24 heures lorsque la pénalité atteint la valeur de 100.

1. Cookie d’Empreinte digitale

Il existe une technique pour prendre les empreintes digitales des utilisateurs de la blockchain en définissant un « cookie d'adresse » sur leur ordinateur.

Un cookie peut vérifier les adresses même lorsque l'utilisateur se connecte via Tor, ou via une chaîne de proxys. Il peut être utilisé pour corréler différentes transactions d'un même utilisateur, même après un redémarrage de l’ordinateur.

Si l'utilisateur décide ultérieurement d'envoyer une transaction non sensible sans Tor, son empreinte digitale peut être corrélée à son adresse IP, désanonymisant ainsi toutes ses transactions envoyées précédemment via Tor.

La technique est basée la découverte des pairs. Chaque adresses de transaction est enregistré dans la base de donnée du réseau par les pairs, et une transaction peut être interrogée.

Model 0x4838B106FCe9647Bdf1E7877BF73cE8B0BAD5f97

1. Questions

qu’est-ce que l’Ethereum ?

À quoi sert-t-il ?

Ethereum est une plateforme de Smart Contract, décrit pour la première fois dans les années 90 par un cryptographe américain, Nick Szabo, dans un papier scientifique publié en 1994 appelé “Smart Contract” : “Un contrat intelligent est un protocole de transaction informatisé qui exécute automatiquement les termes d’un contrat. Un contrat intelligent n’est donc pas un contrat au sens juridique du terme. C’est un accord entre plusieurs parties formalisé sous forme de code informatique, stocké dans une base de données publique. En ce sens, il ne peut être modifié. Lorsque les conditions sont remplies, il permet d’exécuter des transactions de façon automatique sans avoir recours à un tiers de confiance.

où pouvez-vous acheter de l’Ether ?

qu’est-ce qu’un contrat intelligent ?

qu’est-ce que la blockchain ?

comment les donnée d’un block sont elles lues ?

est ce que la blockchain a un sens ?

qu’est ce que le block génome ?

peut-on falsifier un block ?

quel système utilise la blockchain contre la falsification ?

la blockchain a quelque chose qui s’appelle preuve de travail, c’est un mecanisime qui ralentit la creation de nouveau blocks pour calculer la nouvelle preuve de travail, ce mecanisme rend tres difficile la modification des blocs, parce que si vous modifier un bloc vous devrez recalculer la preuve de travail pour tous les bloc suivants.

Mais il y a une autre facon dont les blockchains se securisent et c’est en etant distribué