BTCTKVR edition française



sponsorisée par
SatoshiLabs

contenu

3 Edito de Gritto

4 Affirmer Que Bitcoin Est Un Projet De
10 La NSA Ou De La CIA Est Un Manque De Respect Pour Les Cypherpunks

12 Une Explication Du Réseau Lightning Que
16 Même Un Enfant De 10 Ans Peut Comprendre

18 5 Raisons Pour Lesquelles Vous Devriez Faire
23 Tourner Votre Nœud Bitcoin Sur Un Raspberry Pi 4

24 Elon Musk Ne Saisit Pas Ce Qu'est La
30 Décentralisation, Mais Vous, Vous Devrie

32 Les NFTs Bitcoin Sur Counterparty (Et Comment
45 Obtenir Ou Créer Votre Premier NFT)

46 Raretoshi: Des NFTs Bitcoin Sur
51 La Sidechain Liquid

52 Le Vol De 3094 Bitcoins Qui A Conduit
55 À La CréationDu Trezor

56 Les Bénéfices De Taproot En Matière
60 De Confidentialité

62 Construire Soi-Même Son Hardware Wallet,
66 Partie I :Construisez Votre Trezor One, Model T Et BitBox02

68 Construire Soi-Même Son Hardware Wallet,
74 Partie II

76 Pourquoi Les Bitcoiners Devraient Jouer
78 À Final Fantasy X

80 Comment Je Suis Presque Devenu Riche En
88 Minant Bitcoin Sur SlushPool Pendant Un Mois

90 Le Long Chemin Qui A
94 Mené À Taproot

BTCTKVR

PS

Aucun prix n'a été fixé pour ce magazine car le but premier c'est avant tout de diffuser son contenu au plus grand nombre et son coût d'impression est couvert en partie par nos sponsors (qu'on remercie au passage), mais si vous jugez que ce travail mérite un coup de pouce alors n'hésitez pas à nous soutenir en envoyant le montant qui vous semble juste à l'adresse ci-dessous.

Et voilà, vous tenez entre les main l'édition Française du magazine Bitcoin Takeover. Il s'agit même d'ailleurs à ma connaissance du premier magazine dans la langue de Molière entièrement dédié à la "monnaie magique d'internet". Ces pages représentent le fruit d'un travail commencé il y a plusieurs mois et c'est avec une certaine fierté que je peux enfin vous présenter cette publication franco-roumaine qui je l'espère sera jugée de qualité par ses lecteurs.

Quand on commence à comprendre le changement de paradigme que représente Bitcoin, on ne peut qu'être obsédé par ce dernier et on a rapidement la volonté de donner de son temps libre et de son énergie pour tenter de convaincre ceux qui ne le sont pas encore qu'une révolution positive est en marche. On a tous un rôle à jouer pour démocratiser cette technologie, et c'est un grand plaisir d'apporter cette toute petite pierre à l'édifice gigantesque qui se développe chaque jour un peu plus sous nos yeux à raison d'un bloc toute les 10 minutes.

C'est toujours excitant de voire une nouvelle app qui nous permet de stacker facilement, un nouveau podcast qui nous permet d'entendre certains des génies qui peuplent notre écosystème, un nouveau restaurant qui accepte les sats, etc… Chaque petite initiative quelque soit son domaine ou sa portée s'additionnent et renforcent l'adoption de cette cryptomonnaie indépendante de tout Etat ou leader et c'est dans l'optique d'amener un angle nouveau qu'on a voulu tenter l'expérience de publier un magazine papier.

Tous les articles dans les pages qui suivent ont pour origine la plume de Vlad Costea sur le site Bitcoin Takeover. Si j'affirmais que je suis en accord avec l'ensemble de ses prises de position sans exception, je mentirais un peu, mais rares sont ceux qui avec les 24 heures qui leur sont allouées chaque jours en font autant que lui pour évangéliser le monde au BTC. C'est pourquoi j'ai suivi ce stakhanoviste dans son aventure menant à la publication de ce magazine open source. Et oui, qui dit open source dit qu'il est disponible gratuitement en ligne et que vous pouvez le lire, l'imprimer, le modifier ou même le vendre à votre guise…

Certains des articles retranscrits ici datent d'il y a quelques mois et comme tout va tellement vite dans cet écosystème, certaines informations peuvent potentiellement déjà être légèrement obsolètes ou incomplètes. Mais la substantifique moelle demeure et quel que soit votre niveau d'avancement dans la compréhension de Bitcoin, je suis certains que vous y découvrirez des informations que vous ignoriez.

J'espère que la lecture de ce magazine vous plaira, vous intriguera ou mieux encore vous donnera la volonté d'en savoir toujours plus sur ce protocole et qui sait vous poussera à votre tour à écrire des articles pour partager vos connaissances ou vos opinions sur ce bouleversement aux ramifications tentaculaire.

Bonne lecture, et n'oubliez pas de rester humble et d'amasser des sats !

@Grittoshi



Affirmer Que Bitcoin Est Un Projet De La NSA Ou De La CIA Est Un Manque De Respect Pour Les Cypherpunks

J'ai récemment demandé à mes followers sur Twitter de me soumettre leur théorie du complot favorite concernant Bitcoin. A mon grand étonnement, la plupart des personnes interrogées ont mentionné la thèse selon laquelle la CIA, la NSA ou une autre "agence en trois lettres" sont les créateurs potentiels de la crypto-monnaie.

Deater Bob a suggéré que Satoshi Nakamoto pourrait avoir divulgué le projet Bitcoin à des sources au sein du gouvernement américain. Gilroy a fait état d'un plan machiavélique qui utiliserait les coins de Satoshi comme base d'un nouveau trésor public américain. Des personnes comme Juan Galt ou Jack ont également suggéré que la NSA aurait pu être impliquée.

Et malgré quelques réponses créatives (comme la théorie de Wladimir Van Der Laan selon laquelle Bitcoin serait un champignon ou bien la suggestion de Bmo Masari selon laquelle l'internet lui-même aurait pu atteindre un niveau de conscience lui permettant de créer Bitcoin), je n'ai pu m'empêcher de penser à l'association plutôt répandue qui est faite entre la création de Bitcoin et les agences gouvernementales américaines.

C'est pourquoi, je vais prendre le temps d'expliquer pourquoi cette association est injustifiée – et que quand bien même Satoshi Nakamoto serait la CIA ou la NSA, Bitcoin ne lui/leur appartient plus de toute façon, et que ce projet n'est même pas tout à fait aussi novateur que la plupart des gens l'imaginent.

Bitcoin n'est pas sorti de nulle part et emprunte de multiples avancées que l'on doit aux cypherpunks qui les avaient théorisées et même implémentées parfois bien avant. On doit toutefois reconnaitre à Satoshi Nakamoto, qu'il est celui qui a su créer une solution optimale au problème des généraux byzantins, et qu'il est le



responsable de la mise en circulation d'une forme de monnaie électronique décentralisée nouvelle qui a connu le succès fulgurant qu'on lui connait. On peux ajouter que l'originalité que constitue l'ajustement de la difficulté tous les 2016 blocs qu'il a apporté est également une touche subtile, qui a été cruciale pour la survie du réseau.

Cependant, il existe une tradition cypherpunk qui précède de plus de 20 ans l'émergence de Satoshi. Cet article ne présente toutefois que quelques-unes des inventions qui ont ouvert la voie pour Satoshi sur la manière dont il fallait concevoir Bitcoin et quels écueils avérés il allait devoir éviter.





Satoshi Nakamoto C'est Peut-Être La CIA/NSA, Mais Bitcoin Trouve Ses Racines Dans La Tradition Cypherpunk

De nombreux nocoiners, precoiners ou même bitcoiners mal informés pensent que Satoshi Nakamoto a inventé la blockchain et que tout le mérite lui revient pour ce système comptable qui a par la suite donné naissance à toute une industrie.

Comme beaucoup d'autres inventions cryptographiques, la blockchain a d'abord été conceptualisée par David Chaum pendant son doctorat à l'université de Berkeley. Son Vault System de 1979 comprend même des checks et balances qui ressemblent beaucoup à ceux de Bitcoin : des observateurs (explorateurs de blocs), des exécutants (nœuds), des dirigeants (mineurs), et des "tsars" (développeurs).

Chaum a également créé la première forme de monnaie numérique (ecash) avec la société DigiCash. Elle a été conçue pour résoudre les problèmes de confiance qui se posent avec les paiements en ligne par carte de crédit grâce à une forme de monnaie suffisamment privée pour dissimuler les données personnelles qui ne sont pas utiles à la transaction. Cependant, sa centralisation a finalement conduit à sa disparition à la fin des années 1990. Il est d'ailleurs intéressant de noter que Satoshi ne mentionne pas Chaum dans le livre blanc du Bitcoin.

Mais revenons à la blockchain : l'idée d'une chaîne de hachage qui serait utilisée pour l'horodatage lié est également présentée dans un document de recherche de 1991 par Stuart Haber et W. Scott Stornetta. Et là, contrairement aux travaux de David Chaum, Satoshi fait référence à cette avancée dans le livre blanc de Bitcoin. D'ailleurs, le célèbre bitcoiner Jameson Lopp a cité cette recherche comme annonciatrice de la blockchain de Bitcoin.

Il y a ensuite le choix de l'algorithme de signature numérique à courbes elliptiques (ECDSA), publié en 1998 par les chercheurs canadiens en informatique Don Johnson, Alfred Menezes et Scott Vanstone. Avec ECDSA, des clés publiques, des clés privées et des signatures sont générées afin de garantir que les bitcoins ne peuvent être dépensés

Affirmer Que Bitcoin Est Un Projet De La NSA Ou De La CIA Est Un Manque De Respect Pour Les Cypherpunks
BTCTKVR

que par leurs propriétaires légitimes.

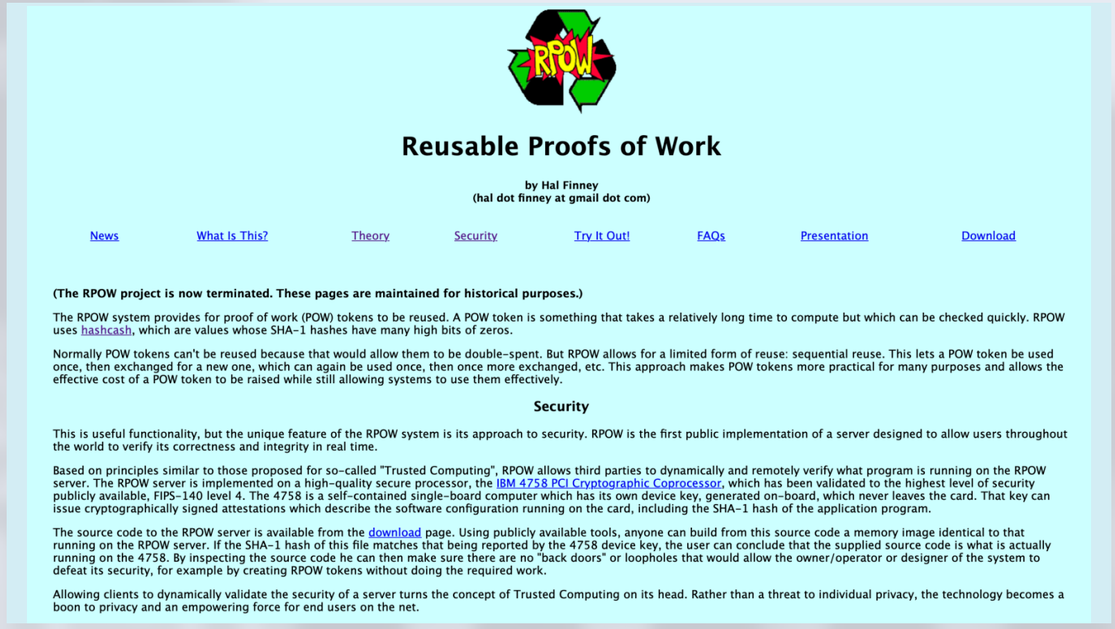
Une théorie populaire voudrait que Satoshi Nakamoto ait choisi ECDSA plutôt que les signatures de Schnorr par commodité, car davantage de bibliothèques étaient disponibles pour répondre à ses/leurs besoins spécifiques lors de la conception de Bitcoin. Pourtant, cela pose de nombreux problèmes de confidentialité (impliquant par exemple la tendance de la NSA à implanter des backdoors) qui mèneront finalement au remplacement de ECDSA par les signatures de Schnorr (merci, Pieter Wuille !).

L'idée d'une cryptographie utilisant des clés publiques n'est pas non plus la propriété de Satoshi Nakamoto : Ralph Merkle effectuait des recherches sur le sujet en 1980 déjà (comme le reconnaît le créateur de Bitcoin dans le livre blanc), et l'outil de messagerie privée PGP de Phil Zimmermann (sur lequel Hal Finney a travaillé pendant de nombreuses années) est disponible gratuitement sur Internet depuis 1991.

Et puisque l'on évoque Hal Finney, Bitcoin utilise sa découverte: la preuve de travail réutilisable (RPOW). Cependant, c'est Adam Back qui est cité dans le livre blanc pour avoir inventé le système hashcash en 1997 et l'avoir perfectionné afin d'empêcher les spams. Sans ces percées cryptographiques, Bitcoin n'aurait jamais pu atteindre le même degré de sécurité – et les brillantes incitations au minage n'auraient probablement jamais vu le jour.

Nick Szabo est un autre illustre cypherpunk qui n'est pas cité dans le livre blanc mais qui avait déjà résolu 90% de Bitcoin. Son système Bit gold reliait déjà avec succès de nombreuses pièces de puzzle parmi les plus brillantes découvertes cryptographiques, et posait également les principes de "l'or numérique" qui sont ancrés dans l'économie autrichienne (rareté, taux d'émission fixe qui évite les pièges de l'hyperinflation, vérification facile).

Malheureusement, la conception de Bit gold reposant sur une majorité de participants au réseau, il pouvait facilement faire l'objet d'attaques 51%. De plus, son taux d'émission (inflation) étant déterminé par le marché, cela signifiait des périodes où davantage de blocs étaient minés, et d'autres où il n'y avait aucune activité et où la sécurité du système était réduite par conséquent. Ce que Satoshi Nakamoto a modifié pour parfaire ce système, a été de remplacer la règle des processeurs par la règle de la puissance de hachage, ainsi que redéfinir comment mettre en place un système financier désinflationniste (commencer avec un taux d'émission élevé, puis le réduire de moitié tous les 4 ans).



Reusable Proofs of Work

by Hal Finney
(hal dot finney at gmail dot com)

News | What Is This? | Theory | Security | Try It Out! | FAQs | Presentation | Download

(The RPOW project is now terminated. These pages are maintained for historical purposes.)

The RPOW system provides for proof of work (POW) tokens to be reused. A POW token is something that takes a relatively long time to compute but which can be checked quickly. RPOW uses hashcash, which are values whose SHA-1 hashes have many high bits of zeros.

Normally POW tokens can't be reused because that would allow them to be double-spent. But RPOW allows for a limited form of reuse: sequential reuse. This lets a POW token be used once, then exchanged for a new one, which can again be used once, then once more exchanged, etc. This approach makes POW tokens more practical for many purposes and allows the effective cost of a POW token to be raised while still allowing systems to use them effectively.

Security

This is useful functionality, but the unique feature of the RPOW system is its approach to security. RPOW is the first public implementation of a server designed to allow users throughout the world to verify its correctness and integrity in real time.

Based on principles similar to those proposed for so-called "Trusted Computing", RPOW allows third parties to dynamically and remotely verify what program is running on the RPOW server. The RPOW server is implemented on a high-quality secure processor, the IBM 4758 PCI Cryptographic Coprocessor, which has been validated to the highest level of security publicly available, FIPS-140 level 4. The 4758 is a self-contained single-board computer which has its own device key, generated on-board, which never leaves the card. That key can issue cryptographically signed attestations which describe the software configuration running on the card, including the SHA-1 hash of the application program.

The source code to the RPOW server is available from the download page. Using publicly available tools, anyone can build from this source code a memory image identical to that running on the RPOW server. If the SHA-1 hash of this file matches that being reported by the 4758 device key, the user can conclude that the supplied source code is what is actually running on the 4758. By inspecting the source code he can then make sure there are no "back doors" or loopholes that would allow the owner/operator or designer of the system to defeat its security, for example by creating RPOW tokens without doing the required work.

Allowing clients to dynamically validate the security of a server turns the concept of Trusted Computing on its head. Rather than a threat to individual privacy, the technology becomes a boon to privacy and an empowering force for end users on the net.

Ces Cypherpunks Avaient Toujours À L'esprit Le Respect De La Vie Privée Et La Résistance À La NSA

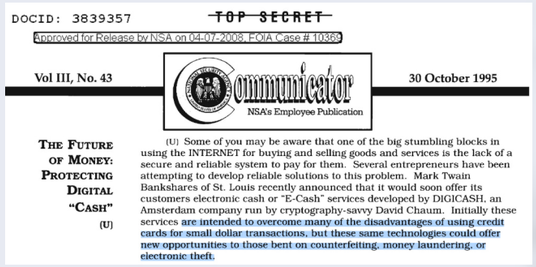
Le terme "punk" dans " cypherpunk" devrait en lui même déjà réussir à démarquer ce mouvement des chaînes gouvernementale. Selon l'opus de 1994 de Tim May, "The Cyphernomicon", les cypherpunks étaient fortement opposés à la surveillance et cherchaient à préserver leur vie privée sur internet tout en inventant des outils pour aider les autres à faire de même.

La conformité en soi était déjà synonyme d'une certaine capitulation idéologique pour eux. David Chaum a écrit "Blind Signatures for Untraceable Payments" en 1983, et "Security Without Identification : Card Computers to Make Big Brother Obsolete" en 1985.Dans un rapport de la NSA datant d'octobre 1995 (qui a été déclassifié depuis en 2008), certaines préoccupations y étaient exprimées quant à la façon dont DigiCash pouvait être utilisé pour des activités criminelles. L'existence de ce document en particulier prouve que les intentions de Chaum étaient authentiques et qu'il était réellement préoccupé par le respect de la vie privée.

Il est hautement improbable que des cypherpunks comme Finney, Szabo, Back, Haber et Stornetta aient pu travailler pour la NSA, la CIA ou toute autre agence gouvernementale. Sinon, leur travail aurait été classifié et leur utilisation restreinte à un personnel autorisé.

Et même en supposant que ce travail open source ait été publié en tant que tel dans le but d'être amélioré par d'autres cryptographes volontaires sur Internet, le fait que ces outils vont à l'encontre des intérêts de monopole intrinsèques à la NSA/CIA, ça donnerait une image de chevaliers au coeur pur de ces cypherpunks.

Si la NSA ou tout autre agence gouvernementale décide d'utiliser le RPOW ou les idées derrière Bit gold pour construire son propre système (ce qui est très probablement déjà arrivé, dans une certaine mesure), cela ne signifie pas pour autant que les inventeurs de ces-dits systèmes étaient leurs employés.



DOCID: 3839357 ~~TOP SECRET~~

Approved for Release by NSA on 04-07-2008, FOIA Case # 10388

Vol III, No. 43 — Communicator, NSA's Employee Publication — 30 October 1995

THE FUTURE OF MONEY: PROTECTING DIGITAL "CASH" (U)

(U) Some of you may be aware that one of the big stumbling blocks in using the INTERNET for buying and selling goods and services is the lack of a secure and reliable system to pay for them. Several entrepreneurs have been attempting to develop reliable solutions to this problem. Mark Twain Bankshares of St. Louis recently announced that it would soon offer its customers electronic cash or "E-Cash" services developed by DIGICASH, an Amsterdam company run by cryptography-savvy David Chaum. Initially these services are intended to overcome many of the disadvantages of using credit cards for small dollar transactions, but these same technologies could offer new opportunities to those bent on counterfeiting, money laundering, or electronic theft.

Bitcoin A Été Inventé Par Satoshi, Mais Il Ne Lui A Jamais Complètement Appartenu

Tout au plus, si Satoshi Nakamoto revenait, il pourrait uniquement déplacer ses coins et les dépenser, rien de plus. Il n'y a pas de backdoor, il n'y a pas de poste de lead developer qui lui est réservé, et il n'y a aucun développeur actif actuellement qui attende le retour du créateur comme le Messie.

Qu'on le veuille ou non, Bitcoin n'est plus le même réseau qu'en 2009. Il a subi de nombreuses améliorations et continuera à laisser l'héritage de Satoshi Nakamoto derrière lui à mesure que d'autres pièces de l'architecture seront remplacées avec le temps.

Après tout, l'intérêt de Bitcoin n'est pas de rester inchangé pour toujours, mais de conserver sa politique monétaire, de garantir que Satoshi puisse revenir à tout moment pour déplacer ses coins, et de préserver la décentralisation.

Satoshi Nakamoto a fait énormément de bonne choses, mais il a également produit une quantité de code qui a été supprimé ou remplacé par les développeurs par la suite. Hal Finney a passé beaucoup de temps à corriger les défauts de conception de Bitcoin (il est même responsable de l'ajout des zéros supplémentaires pour définir la plus petite unité monétaire du système comme 1/100 000 000 BTC) et il a créé un précédent pour les futurs développeurs en cherchant des solutions plus élégantes et efficaces pour ce projet bien plus rigide au départ.

Bitcoin en tant que système monétaire est gravé dans la marbre avec son offre fixe, son inflation prévisible jusqu'en 2140, ses récompenses pour le minage limpides et ses ajustements de la difficulté tous les 2016 blocs. Mais Bitcoin en tant que réseau était destiné dès le départ à accueillir de nombreuses améliorations qui allaient le rendre plus rapide, plus privé et plus efficace.

Les propositions d'amélioration telles que les signatures de Schnorr, Taproot, MAST ou Grafroot sont conçues par exemple pour améliorer la confidentialité et l'efficacité des blocs (transactions plus petites et plus abordables).

Ensuite, de nombreuses améliorations qui ont attrait à la confidentialité sont à l'étude sur d'autres réseaux d'altcoins ou sur les sidechains (ce n'est vraisemblablement qu'une question de temps avant que les Confidential Transaction ou MimbleWimble ne soient ajoutées à la couche de base dans une certaine mesure). À l'avenir, il est fort probable que la confidentialité des transactions devienne plus populaire, et que des astuces ingénieuses garantissant toujours l'auditabilité de l'offre et la résistance à l'inflation soient mises en œuvre.

Si Satoshi revenait aujourd'hui, il ne reconnaîtrait probablement pas sa propre invention. Et c'est sans doutes très bien ainsi, car le réseau se développe et devient bien plus efficace dans l'optique de son objectif premier. Bitcoin est comme une voiture de sport qui reçoit de multiples améliorations sous le capot sans jamais changer de carrosserie – elle conservera toujours ses qualités principales de conception, mais en l'améliorant avec un moteur plus performant et des vitres blindées.





Même Si Satoshi Nakamoto C'est a NSA/CIA, Bitcoin Ne Leur Appartient Pas De Toute Façon

Bitcoin a-t-il été conçu par une des agences à trois lettres? C'est tout à fait possible. La CIA et la NSA pourraient-elles utiliser Bitcoin pour certaines transactions? C'est encore plus probable. Mais aucune de ces deux assertions ne mène à la conclusion qu'une de ces agence gouvernementale est aux commandes de Bitcoin aujourd'hui.

À l'heure actuelle, Bitcoin est peut-être le réseau informatique le plus décentralisé de la planète. Il fonctionne depuis janvier 2009 et n'a connu que deux interruptions (dues à un bug d'inflation en 2010 et à une mauvaise synchronisation du réseau en 2013). Il compte plus de 15 000 nœuds dans le monde (sans compter l'ensemble de ceux qui fonctionnent sur Tor et ceux qui n'ont pas ouvert le port 8333).

Certains affirment que des backdoors peuvent exister et que le plus grand dommage qu'elles pourraient causer serait de casser les signatures (ce qui pourrait conduire au vol des fonds) ou de casser la cryptographie derrière SHA256. Dans les deux cas, de toute façon, il serait possible pour la communauté de passer sur une nouvelle chaîne, de remplacer ECDSA et SHA256 par des alternatives existantes qui ont déjà été développées, et de restaurer la propriété des coins précédents sur la base de preuves cryptographiques. Cette solution parait certes impopulaire aujourd'hui, mais pourrait s'avérer être le dernier recours en cas d'attaque sérieuse d'un type auquel Bitcoin n'a jamais encore été confronté.

La bataille contre Big Brother est implacable, et il est clair que les responsables gouvernementaux comprennent les compromis que cela impliquerait de lancer des attaques ou manquent peut-être simplement momentanément de moyens pour les engager. Il est également probable que la CIA et la NSA trouvent l'existence de



Bitcoin pratique, puisqu'elles l'utilisent elles-mêmes et disposent de leurs propres moyens pour suivre les transactions sur la blockchain en examinant les communications entre les participants et d'autres indices au niveau du réseau.

Mais même si l'on suppose que Satoshi Nakamoto était le chef d'orchestre d'une poignée d'agents de la CIA, l'expérience lui a clairement échappé et il n'en a plus le contrôle – et il ne l'aura manifestement plus jamais, à moins que le réseau ne redevienne plus centralisé (comme cela a pu se produire avec BCH ou BSV).

Et quand bien même la moitié de la communauté Bitcoin serait à la solde de la CIA, l'autre moitié peut toujours résister aux attaques en migrant sur une autre chaîne qui conserve les règles mais change les mécanismes de sécurité. Il s'agit d'un logiciel open-source et les moyens de protéger la propriété de chaque entité doivent être défendues.

Et en vérité, grâce aux brillantes incitations du réseau, il est préférable pour tout le monde (agents de la CIA ou non) de se serrer les coudes et de protéger le même réseau. Aussi longtemps que l'appât du gain fonctionnera, Bitcoin restera sûr et méfiant envers les entités qu'il verra rejoindre son réseau.

La devise "don't trust, verify" fait principalement référence à la validation par d'autres personnes et implique la possession de son propre nœud comme moyen tangible de prouver que les fonds existent bien et vous reviennent de droit. Par conséquent, il s'agit de partir du postulat selon lequel tout le monde a pour seul et unique but de vous voler – parce que c'est bien connu: tout le monde est un escroc ("everyone's scammer").

Mais Euuuh Satoshi

Le Satoshi Nakamoto que nous connaissons grâce aux messages sur le forum Bitcointalk et à la cypherpunk mailing list était plutôt humble et terre-à-terre. Il était prêt à prendre du temps pour aider quiconque à comprendre le fonctionnement de Bitcoin (à l'exception notable de Daniel Larimer qui s'est fait remballé d'une manière assez musclée – le fameux "if you don't believe me or don't get it, i don't have time to try to convince you, sorry").

Cependant, le transformer en une sorte de figure messianique qui nous a donné le pouvoir du Saint-Esprit et est parti pour revenir un jour est définitivement une erreur. On ne peut pas nier les contributions de Satoshi au monde de la cryptographie, mais on ne doit pas non plus exagérer son travail.

Bien entendu, l'histoire du programmeur informatique inconnu qui a lancé un système innovant de monnaie numérique sorti de nulle part peut apparaitre romantique. Elle attire les nouveaux venus et occupe les médias avec de fausses enquêtes. Pourtant, le génie de Satoshi Nakamoto est un peu exagéré et il n'a finalement pas ajouté grand-chose aux inventions autrement plus impressionnantes mais pourtant moins populaires de ses pairs.

C'est l'exemple classique d'Isaac Newton et de son ami Wilhelm Leibniz : tout le monde connaît le premier avec son histoire de pomme, mais on a tendance à oublier le second. Ils ont tous deux découvert le calcul intégral à peu près au même moment, mais la gloire semble pourtant injustement pencher énormément du côté du polymathe anglais.

En définitive, l'identité de Satoshi Nakamoto importe peu et est quasiment dépourvue d'intérêt à ce stade du développement de Bitcoin. De plus, toutes ces histoires de NSA /CIA sont plutôt regrettables quand on a conscience des origines ouvertement cypherpunk de Bitcoin. En bref et pour conclure, même si on veut admettre que Satoshi ait pu être la NSA, Bitcoin lui ne l'est clairement pas.

vaultoro.com

Vaultoro

Économisez en actifs tangibles,
construisez votre patrimoine

Achetez et vendez de l'or et de l'argent grâce aux crypto-monnaies avec des commissions avantageuses, de manière sure et garantie, dans des chambres-fortes professionnelles en Suisse.

vaultoro.com



Une Explication Du Réseau Lightning Que Même Un Enfant De 10 Ans Peut Comprendre

En tant que seconde couche de Bitcoin, le réseau Lightning apporte de nombreuses améliorations. Il permet des paiements quasiment instantanés accompagné d'une mise à l'échelle qui permet d'atteindre une capacité qui n'a rien à envier à Visa par exemple et, cerise sur le gâteau: il est plutôt privé. Il peut également permettre de faire tout ce que des altcoins comme Ethereum par exemple font actuellement (NFTs, DeFi, tokenization, smart contracts avancés), mais d'une manière plus "élégante" et plus rentable.

Pourtant, en dépit de ses avantages multiples, nombreuses sont encore les personnes qui n'adhèrent pas au réseau Lightning, parfois tout simplement parce qu'elles ne comprennent pas sa nature, la manière dont il fonctionne ou bien tout simplement comment elles peuvent y participer. Afin de faciliter la compréhension de tous, je vais tenter d'expliquer la terminologie essentielle inhérente à ce réseau, en me servant d'exemples pratiques et d'analogies. Et normalement, si vous avez plus de 10 ans, vous devriez comprendre.

Vous Avez Besoin De Vos Propres Nœuds Bitcoin & Lightning

Tout d'abord, afin de profiter pleinement du Lightning Network, vous allez devoir faire tourner votre propre nœud. On vit dans un monde décentralisé, en on s'efforce de bâtir des produits et des services qui ne reposent sur aucuns tiers de confiance. Dans l'idéal, vous devriez acheter du matériel que vous allez spécifiquement dédier à votre nœud – et si c'est votre souhait vous pouvez déjà compter sur des solutions pré-construites comme :

- RaspiBlitz (environ 319€, qui bénéficie d'une distribution européenne et américaine) ;
- MyNodeBTC (environ 429$, que vous pouvez acheter sur leur site) ;
- Nodl (529$, que vous pouvez l'acheter sur leur site) ;
- Start9 Labs Embassy (environ 289$, disque dur non-inclus, mais qui n'est plus disponible actuellement).

Si vous souhaitez réduire ces dépenses et réaliser un beau projet de bricolage DYI sympa pendant vos week-end, vous pouvez aussi choisir d'acheter un RaspBerry Pi 4B avec 4 Go de RAM, un SSD de 1 To de votre choix (se concentrer sur ceux des marques fiables), une carte SD de 32 Go, un boîtier de dissipation thermique pour garder votre RaspBerry Pi au frais pendant les étés et les processus gourmands en ressources, et quelques câbles. Il vous suffira ensuite par exemple de regarder le tutoriel étape par étape de Ben Arc sur YouTube (BTCIOT Tutorial – Raspiblitz LN Node) afin d'appréhender clairement les différentes actions que vous allez devoir effectuer pour faire fonctionner votre RaspiBlitz.

Si en revanche vous ne voulez pas mettre de l'argent dans un dispositif spécifiquement dédié à ça, il existe au moins deux manières assez répandues de faire tourner un nœud Lightning sur votre ordinateur. La plus avancée nécessitera l'utilisation du wallet Electrum (un guide complet est disponible sur le forum Bitcointalk), et la seconde, qui s'avère être plus basique et plus user-friendly, sera de vous aventurer sur Linux avec Umbrel. Et si toutefois vous vous sentez prêt à relever un défi encore plus conséquent, vous pouvez également choisir de faire tourner un RaspBerry Pi OS sur votre ordinateur Windows ou Mac ou même vous orientez vers les machines virtuelles.

Mais la recommandation d'utiliser un appareil spécifiquement dédié est motivée par des raisons d'efficacité et de sécurité : le RaspBerry Pi consomme très peu d'électricité et est respectueux de l'environnement (son fonctionnement 24 heures sur 24 et 7 jours sur 7 ne vous coûtera que quelques euros par an), et un appareil qui n'effectue qu'une seule tâche précise présente une surface d'attaque bien plus faible qu'un appareil qu'on utilisera aussi au hasard pour ouvrir des emails, installer des logiciels tiers ou bien accéder à des pages Web "douteuses".

Donc si vous avez la possibilité de mettre la main sur un RaspBerry Pi pour faire tourner votre nœud, vous devriez le faire. Ce n'est certes pas très abordable pour le moment, mais c'est appelé à s'améliorer avec le temps, à mesure que la technologie prendra de l'âge et que nous disposerons de matériel plus rapide et plus innovant.

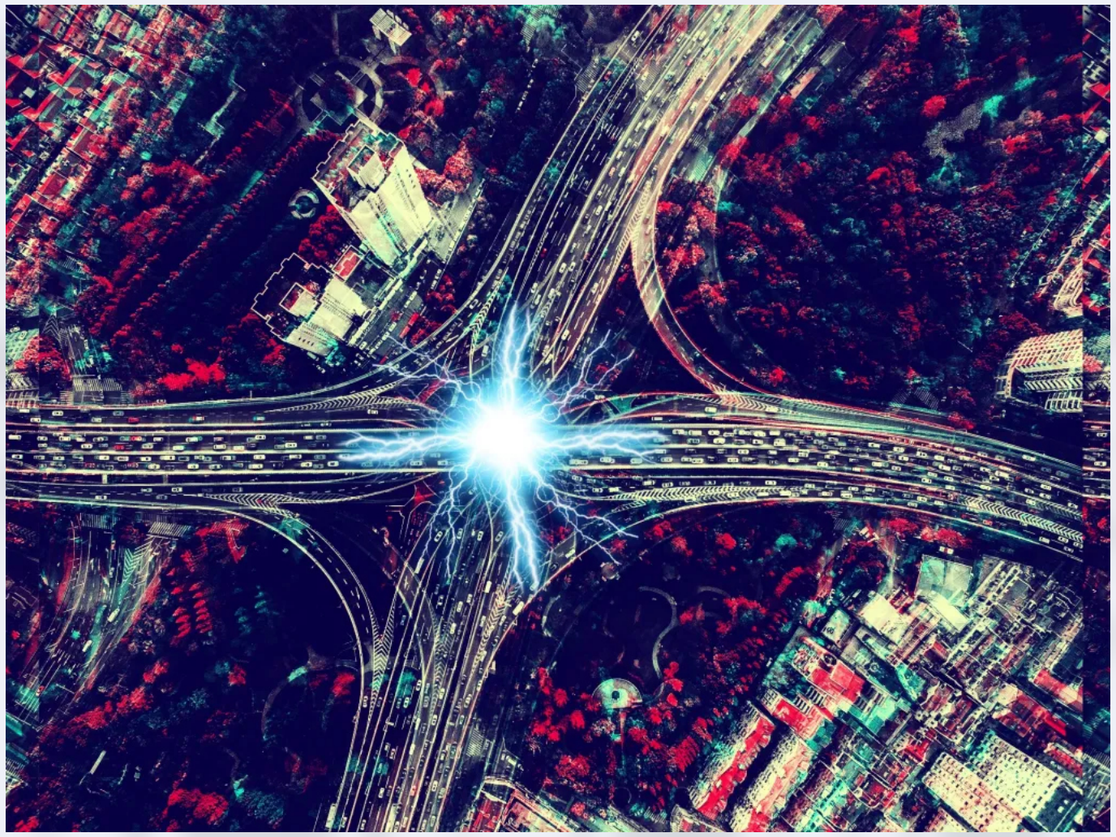
Les Nœuds Lightning Sont Des Îles, Les Canaux Sont Des Routes

Une des idées fausses la plus répandue à propos du Lightning Network est qu'il suffirait de faire tourner un nœud pour être connecté au reste du réseau. Bien que le nœud soit certes un pré-requis essentiel, il faut ajouter une étape additionnelle à votre périple et celle-ci consiste à ouvrir des canaux avec d'autres personnes.

Pour mieux comprendre le concept, essayez d'imaginer que votre nœud est une île qui viendrait d'émerger au milieu d'un océan. Votre objectif désormais est de construire des routes sur des ponts qui mèneront à toutes les personnes avec lesquelles vous allez effectuer des transactions. Plus il y aura de routes plus cela signifiera que vous aurez de connexions et de meilleurs raccourcis vous permettant d'atteindre certaines destinations.

La taille de vos canaux est également importante, car ils permettent d'effectuer des transactions plus ou moins importantes. C'est un peu comme si votre pont menant vers une autre île ne permettait qu'aux véhicules d'un certain tonnage de circuler – plus le pont sera solide, plus il sera capable de supporter de poids au cours d'un seul voyage.

Ces routes sont à double sens : vous pouvez les construire en direction d'autres îles (ça augmentera votre capacité d'envoi) ou d'autres îles peuvent les construire en votre direction (et ça augmentera votre capacité de réception). Pour avoir une île bien connectée on aura besoin des deux.



Quand vous allez envoyer de l'argent vers n'importe quelle île de la carte, vous allez devoir emprunter l'une des routes existantes. Si vous avez une route directe, alors c'est tout est simple et vous pouvez effectuer votre transaction en fonction de la taille de votre canal. Mais si vous et le destinataires devez nécessairement emprunter la route d'un tiers pour être reliés l'un à l'autre, alors vous allez devoir payer des "frais d'itinéraire" pour utiliser ces routes (en gros on peut voir ça comme un péage).

Dans l'idéal, vous devriez donc ouvrir des canaux avec chaque nœud du réseau pour toujours avoir des connexions directes – mais c'est peu pratique et concrètement quasi-impossible à réaliser à mesure que le réseau croit. Lorsque des millions de bitcoiners ouvriront au moins un canal par jour, il sera plus que difficile de disposer des fonds, du temps et de l'énergie nécessaires pour suivre la croissance du réseau Lightning. Mais pas de panique car le routage demeure très efficace et possède également des avantages en matière de confidentialité. En effet, comme dans le cas du réseau Tor, chaque nœud relais ajoute une couche supplémentaire de cryptage et d'anonymat.

Quand vous construisez des routes, vous pouvez vous aussi percevoir des frais de péage auprès de ceux qui utilisent votre infrastructure pour se rendre à leur destination. Servir d'intermédiaire pour d'autres transactions peut présenter des avantages financiers, et la plupart des gestionnaires de portefeuilles Lightning vous donnent la possibilité de choisir le montant que vous souhaitez prélever à ceux qui utiliseront votre route. Gardez toutefois à l'esprit que c'est généralement la route la plus courte, la plus rapide et la moins chère qui sera privilégiée. Donc, à moins de relier des îles obscures ignorées de tous les autres, vous devriez y réfléchir à deux fois avant de fixer un tarif élevé. Avec une grande quantité de transactions, ces micro-revenus s'additionneront et devraient arriver à subventionner les coûts énergétiques



qu'implique le fonctionnement de votre nœud.

Des gestionnaires de réseaux Lightning tels que RTL (Run the Lightning) vous permettent d'ouvrir des canaux privés si vous le souhaitez. Ça signifie pour schématiser que seuls vous et le nœud avec lequel vous avez établi un pont peuvent voir et utiliser cet élément d'infrastructure. Bien que cela puisse présenter certains avantages en termes de confidentialité (personne d'autre n'est au courant), la contrepartie est qu'aucune autre transaction n'empruntera jamais votre route et que par conséquent vous ne soutenez pas vraiment le réseau et vous ne toucherez aucuns de frais de routage/péage.

La taille de vos canaux (ou la résistance au poids de vos routes/ponts comme nous l'avons défini plus tôt) n'est pas permanente et vous pouvez faire des rééquilibrages afin d'augmenter ou réduire certaines capacités. Vous allez assurément devoir payer des frais pour ce type d'opération, mais il est sain de sans cesse garder un œil sur les opérations en cours afin de pouvoir privilégier telle ou telle route en fonction de votre observation. Octroyer une plus grande capacité à vos routes les plus populaire et les plus utilisées vous sera bénéfique.

Enfin, et c'est loin d'être négligeable, n'oubliez pas que les canaux sont plus faciles à démanteler que des routes. En cliquant simplement sur un bouton, vous pouvez fermer le canal et ramener vos fonds sur la couche de base de Bitcoin. Chaque fois que vous ouvrez un canal, vous payez des frais de transaction aux mineurs Bitcoins, et il en est de même lorsque vous fermez des canaux. Pour éviter de surpayer ces opérations, il existe des guides disponibles en ligne sur les différents façons de vous acquitter de frais de transaction moins élevés.

Les Clients De Lightning : LND, C-Lightning, Eclair & Nayuta

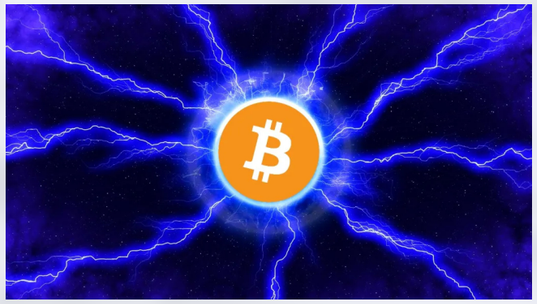
Tout comme les routes peuvent être construites à partir de différents matériaux qui ont leurs avantages et leurs inconvénients, le client de référence Lightning compte quatre versions qui ont aussi leurs propres avantages et inconvénients. Historiquement, LND de Lightning Labs est l'implémentation la plus populaire et c'est par exemple celle qui est utilisée par les systèmes d'exploitation des nœuds RaspBerry Pi (à l'exception notable d'Embassy de Start9 Labs, qui est également fourni avec c-lightning). Grâce à son large éventail d'applications et l'effet de réseau, il s'agit du plus abordable pour les utilisateurs inexpérimentés.

C-lightning de Blockstream est plus "raffiné" et mieux adapté aux développeurs, et il est construit dans le langage de programmation C (d'où son nom). Cependant, il possède moins d'applications et reste aujourd'hui surtout utilisé par les exchanges et les services qui nécessitent une fiabilité plus conséquente. Elle est également conçue de façon à permettre des atomic swaps entre les différents actifs de la sidechain Liquid de Blockstream et BTC Lightning. Ça peut s'avérer utile si vous souhaitez effectuer un peg-out sans utiliser les services KYC d'un exchange de la fédération Liquid. Si on comparait LND à Windows, alors c-lightning serait une distribution Linux, robuste mais qui aurait le défaut de n'être n'est pas très abordable par des utilisateurs lambdas peu doués techniquement.

Eclair de ACINQ s'avère aussi une option assez populaire, entre autre parce qu'elle est écrite en Scala et prend en charge les plug-ins Java et Java Virtual Machine. Or, comme de nombreuses applications Android OS sont écrites en Java, cette implémentation peut se révèler très utile pour les wallets disponibles sur les téléphones portables. Phoenix et Eclair sont d'ailleurs deux des wallets les plus populaires pour mobiles, et il est vivement conseillé de les essayer, si ce n'est déjà fait.

Enfin, il y a Nayuta, une société japonaise qui

a commencé à travailler sur un client Lightning si léger que même un RaspBerry Pi Zero peut le faire tourner. Plus récemment, elle a publié une version alpha de Nayuta Core et se concentre également sur le développement de wallets pour mobiles.



L'option La Plus Simple Pour Se Laisser Électriser Par Lightning

Idéalement, vous devriez gérer votre propre nœud et tout bien faire dans les règles. Mais si dans un premier temps vous souhaitez uniquement vous familiariser un peu avec Lightning et son fonctionnement, vous pouvez déjà essayer un wallet pour mobile comme Blue Wallet, Breez ou bien Eclair.

Blue Wallet est le portefeuille qui remporte la palme en terme d'expérience utilisateur entre tous les wallets Bitcoin confondus.

Il est également très personnalisable, vous permettant soit de vous connecter à votre propre nœud, soit de vous reposer sur l'infrastructure de l'entreprise.

Et si vous souhaitez recevoir un paiement Lightning, vous installez l'application sur votre téléphone, vous générez une facture pour le montant que vous souhaitez recevoir, puis il ne vous restera plus qu'à vous laisser surprendre par la vitesse de la transaction.

Blue dispose également d'une version desktop, ce qui en fait l'un des moyens les plus pratiques pour commencer à utiliser le réseau Lightning.

Le Breez Wallet est spécial dans la mesure où il ouvre un canal pour vous. Après avoir déposé des fonds et attendu 3 confirmations du réseau minimum, tout est prêt.

Le fait que cette expérience utilisateur simple se déroule d'une manière non-custodial, renforçant donc votre souveraineté, est vraiment positif.

Ce n'est certes pas comparable à l'expérience qui peut découler d'un nœud complet, mais ça promeut tout de même les avantages offerts par Lightning grâce à quelques compromis élégants.

Et puis il y a Eclair Mobile de ACINQ, qui fait tourner une version légère d'un nœud Lightning directement sur votre téléphone mobile. Il vous offre également la possibilité de vous connecter à votre propre full node en allant modifier les paramètres avancés.

Lightning Network

Scalable, Instant Bitcoin/Blockchain Transactions

Mais même si l'on se cantonne aux paramètres par défaut, ce wallet demeure une excellente option sur le plan de la souveraineté financière.

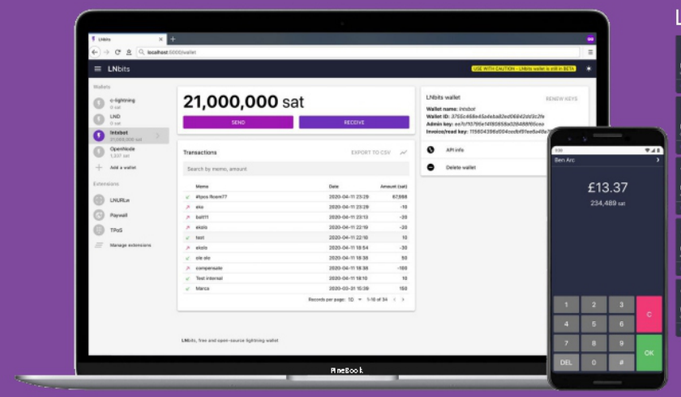
Ça aurait été formidable qu'il soit également disponible sur iOS, mais ce n'est malheureusement pas le cas, probablement en raison des limitations des produits Apple. Par contre, si vous avez une carte SD suffisamment grosse, vous pourrez même exécuter un full validating node sur votre téléphone.

Enfin, si vous cherchez un moyen de recevoir vos premiers fonds sur le Lightning Network sans effort, vous pouvez simplement vous inscrire à des services de tips et de paiement sur les réseaux sociaux tels que Tippin.me ou Bottle Pay.

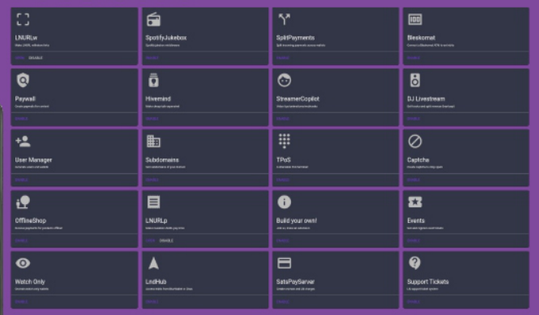
Par la suite, si vous avez des fonds sur le Lightning Network que vous devez "rapatrier" sur la chaîne principale de Bitcoin et que vous n'avez pas de canaux à fermer parce que vous êtes full-custodial, un service comme ZigZag pourra vous aider dans cette tâche.

LNbits

Système de comptes bitcoin et extensions, gratuit et open source.
Sur ta node, à partager avec ta famille, tes amis, ou le monde entier!



LNbits extensions:



Sats gratuits!
(Scanne avec un portefeuille bitcoin lightning)

Coinflip!
(Scanne avec un portefeuille bitcoin lightning)

LNbits, c'est WordPress pour ta node lightning, avec une douzaine d'extensions géniales pour améliorer ta node comme tu le souhaites. LNbits peut à la fois être:

- un portefeuille personnel pour comptes lightning
- un service de gestion "custodial" pour le monde entier
- une solution pour banques locales
- un portefeuille instantané parfait pour les nouveaux utilisateurs
- un outil puissant à inclure dans ta suite logicielle

LNbits can run on:

RASPIBLITZ Clightning LND
LNPay.co LNTXbot myNode
opennode spark Umbrel

Rejoignez-nous! https://github.com/lnbits/lnbits



5 Raisons Pour Lesquelles Vous Devriez Faire Tourner Votre Nœud Bitcoin Sur Un Raspberry Pi 4

Les nœuds Bitcoin sont les validateurs du réseau : ils s'assurent que les mineurs restent honnêtes et ils permettent aux utilisateurs de vérifier leurs propres transactions, tout en leur permettant une maîtrise relative de la confidentialité de leurs finances. Ils sont un outil de souveraineté capable de fonctionner sur à peu près n'importe quel ordinateur produit depuis 2010. Et dans ce contexte, le Raspberry Pi demeure un choix de prédilection en tant que matériel de validation, et ce pour de nombreuses raisons.

Je précise tout d'abord que cet article n'est en aucun cas rémunéré ou soutenu par la Fondation Raspberry Pi et n'a pas pour vocation de vous convaincre à acheter un nouvel appareil. En réalité, l'ordinateur idéal que vous pouvez utiliser pour faire tourner un nœud Bitcoin, c'est celui que vous possédez déjà. Toutefois, il existe des avantages indéniables à utiliser ces petites machines ARM.

Certes, les versions précédentes étaient lentes et pas vraiment fiables. Lorsque j'ai testé le Casa Node qui tournait sur un Raspberry Pi 3 en février 2019, il décevait par sa lenteur. La plupart du temps, je n'avais même aucune idée si l'appareil était figé ou bien si je devais attendre un peu plus longtemps pour qu'il finisse de charger ses donnés. Mais plus tard dans l'année, le Raspberry 4 a été lancé sur le marché et il a dévoilé ses processeurs quad-core bien plus rapides, ainsi que ses 4 gigaoctets de RAM – et tout ça pour un prix de 50 euros.

Porté par ces avancées au niveau du microprocesseur et des économies d'échelle, devenir financièrement souverain n'a jamais été aussi facile, ni aussi abordable. Donc sans s'appesantir plus longuement sur l'introduction, voici 5 raisons pour lesquelles vous devriez faire tourner votre nœud Bitcoin sur un Raspberry Pi 4.

1. Le Raspberry Pi 4 Est Économe En Énergie Et Écologique

Face à tous les commentaires fallacieux du type "Bitcoin fait bouillir les océans", il est bon d'avoir l'antithèse avec un réseau Bitcoin qui fonctionne grace à un appareil aussi peu énergivore. Laisser tourner 24 heures sur 24 et 7 jours sur 7 votre nœud Bitcoin Raspberry Pi 4 ne consommera pas plus d'énergie que le chargement quotidien de votre iPhone. Et ce n'est pas un mince exploit, car ainsi des millions d'utilisateurs peuvent accéder à la possibilité de faire tourner leur propre noeud de validation Bitcoin grâce aux coûts d'entretien et de fonctionnement réduits à leur minimum.

À aucun moment, mes noeuds Bitcoin et Ligthning Raspberry Pi 4 n'utilisent plus d'un tiers de la puissance de calcul de l'appareil. Cela signifie que la consommation d'énergie oscille aux alentours de 4 watts environ (soit un kilowatt toutes les ~24 heures; donc environ 365 kilowatts par an). Au tarif de 75 centimes par kilowatt chez mon fournisseur d'énergie actuel, faire tourner le nœud 24 heures sur 24 et 7 jours sur 7 me revient ainsi à 27 euros par an environ.

Le fait que je l'utilise pour faire tourner à la fois les réseaux Bitcoin et Lightning est encore plus impressionnant. Et si on tient compte du fait que les transactions Lightning actuelles sont traitées pour un très grande nombre par des Raspberry Pi, on peut sans doute affirmer que cette deuxième couche est aujourd'hui le moyen le plus écologique pour envoyer de l'argent sur cette planète.



2. Le Raspberry Pi 4 Est Bon Marché, Polyvalent Et Il Est Facile De Se Le Procurer Partout Dans Le Monde

Si les rigs de minage peuvent facilement coûter quelques milliers d'euros, l'achat d'un nouveau Raspberry Pi 4 avec un disque dur de grande capacité, un boîtier isotherme, un écran tactile et des câbles ne s'élève en théorie pas à plus de 175 euros. Dans cette configuration, c'est en fait le disque dur de 1TB qui sera le plus cher (surtout si vous optez pour un SSD plus rapide et plus silencieux).

En outre, l'engouement pour le Raspberry Pi a permis d'augmenter sa disponibilité et ses cas d'usage de manière globale. Vous pouvez donc maintenant entrer dans le magasin d'électronique du coin (ou aller sur le site web d'un revendeur) et acheter l'un de ces petits appareils ARM avec une bonne dose de "déni plausible". Si votre gouvernement autoritaire vous pose la question, vous pouvez tout simplement prétendre que vous voulez en faire une console de jeux vidéo ou un ordinateur de bureau ordinaire – ces deux cas d'utilisation sont répandus et plausibles; ça ne suscitera absolument aucuns soupçons.

Dans le cas du matériel Bitcoin, il est important qu'il ne soit pas spécifique à celui-ci ou étiqueté comme tel. S'ils venaient à savoir que des unités d'or numérique constituent la récompense potentielle, des individus malveillants seraient grandement incités à compromettre votre appareil durant les étapes d'acheminement de ce dernier. Toutefois les cas d'utilisation les plus courants des Raspberry Pi demeurent ceux n'impliquant pas Bitcoin. Donc, pour vous offrir une possibilité supplémentaire de nier les faits de façon plausible, vous pouvez même aller jusqu'à acheter deux appareils et utiliser l'un d'eux pour le cas d'utilisation le plus courant et attendu. Grâce à cet artifice, la probabilité d'une attaque de la chaîne d'approvisionnement diminue considérablement (ça ne signifie pas pour autant que vous devez négliger de procéder à une vérification de la puce vous-même).

3. Beaucoup De Logiciels Bitcoin Fonctionnent Avec Le Raspberry Pi 4

La valeur d'un matériel informatique est proportionnelle aux logiciels qui utilisent ses capacités. Pour ce qui est de Bitcoin, il existe une multitude d'options robustes, gratuites et open source destinées aux noeuds Raspberry Pi. Depuis la création de RaspiBolt par Stadicus, on a pu assister à tout une vague de systèmes d'exploitation faciles à utiliser et qui permettent de faire tourner les réseaux Bitcoin et Lightning sur du matériel abordable.

Je recommande généralement aux gens d'utiliser RaspiBlitz, car il offre une grande quantité de fonctionnalités et d'extensions en plus d'un interface utilisateur minimaliste mais bien rédigé. Il existe toutefois plusieurs autres excellentes options telles que MyNode ou Embassy OS de Start9 Labs. Une autre option très populaire est Umbrel, mais sa licence n'étant pas celle spécifique aux logiciels libres et open source (du moins pas encore), je ne saurais le recommander pour l'instant.

Si je devais faire des comparaisons ces solutions avec les systèmes d'exploitation des ordinateurs de bureau, RaspiBolt serait Debian Linux, RaspiBlitz serait Ubuntu, MyNode serait Mint Linux, Embassy OS de Start9 Labs serait Red Hat Linux, tandis que Umbrel serait Mac OS.

Quel que soit celui que vous choisissez, vous y trouverez en commun quelques uns des logiciels très performants. Cela inclut Electrum Server, Run the Lightning, BTCPay Server, l'intégration de Tor, LNBits, un service de mixage tel que JoinMarket et une application de chat décentralisée telle que Sphinx (entre autres).

Tous ces logiciels vous offrent un moyen sûr et compréhensible d'accéder aux applications Bitcoin et Lightning sur un Raspberry Pi, tout en conservant tous les avantages d'un citoyen de premier ordre du réseau Bitcoin. La validation de vos propres transactions, la génération d'adresses de réception à partir d'une clé xpub auto-hébergé, l'ouverture de vos propres canaux Lightning et la gestion de vos propres clés privées font toutes partie de cette expérience, certes un peu technique, mais tellement enrichissante.

C'est complètement fou quand on y pense que le Raspberry soit capable d'offrir une expérience Bitcoin plus dense et plus efficace que les ordinateurs personnels fonctionnant sous Windows ou MacOS.



4. Le Raspberry Pi 4 Est Tout Petit Et Silencieux

Beaucoup de choses peuvent êtres dites en ce qui concerne les avantages de ce petit ordinateur, mais l'un de ses principaux atouts qui se dégage reste celui de pouvoir être placé dans son salon sans avoir à se soucier du bruit si jamais vous décidiez de l'avoir constamment en activité.

Si en plus vous ajoutez un boîtier aluminium de bonne qualité et qui dissipe efficacement la chaleur, vous n'aurez même pas à opter pour des solutions bruyantes de refroidissement actif. Et si vous faites tourner vos nœuds Bitcoin et Lightning sur un SSD, il n'y aura rien qui tournera dans le vide ou fera du bruit. Vous aurez affaire à l'expérience la plus silencieuse, la moins onéreuse et la plus respectueuse de l'environnement qui soit.

En plus, comme il se présente sous la forme d'un boîtier pas plus grand que la main, vous pourrez facilement le glisser derrière un meuble, et ceci contribue aussi à la protection de votre vie privée, au déni plausible encore une fois et par extension à votre sérénité.



5. Le Raspberry Pi 4 Est Plutôt Sûr Quand Il Est Dédié À Un Nœud Bitcoin

Les gens utilisent des ordinateurs Raspberry Pi pour faire tourner des serveurs, des relais, des émulateurs de jeux vidéo, des machines de livestreaming, des processeurs de paiement et la killer app, celle qui les domine tous : la validation des transactions Bitcoin et Lightning (et ce n'est pas faute de pouvoir le faire sur un ordinateur plus puissant faisant tout tourner dans des machines virtuelles)

L'enjeu c'est la sécurité : si vous disposez d'un appareil qui n'effectue qu'une seule tâche spécifique et que l'ensemble son matériel est optimisé pour ça, alors sa surface d'attaque est bien plus réduite. En revanche, en raison d'une plus grande complexité de paramétrage, un ordinateur de travail multi-core capable de tout faire tourner dans des machines virtuelles est largement plus vulnérable aux attaques.

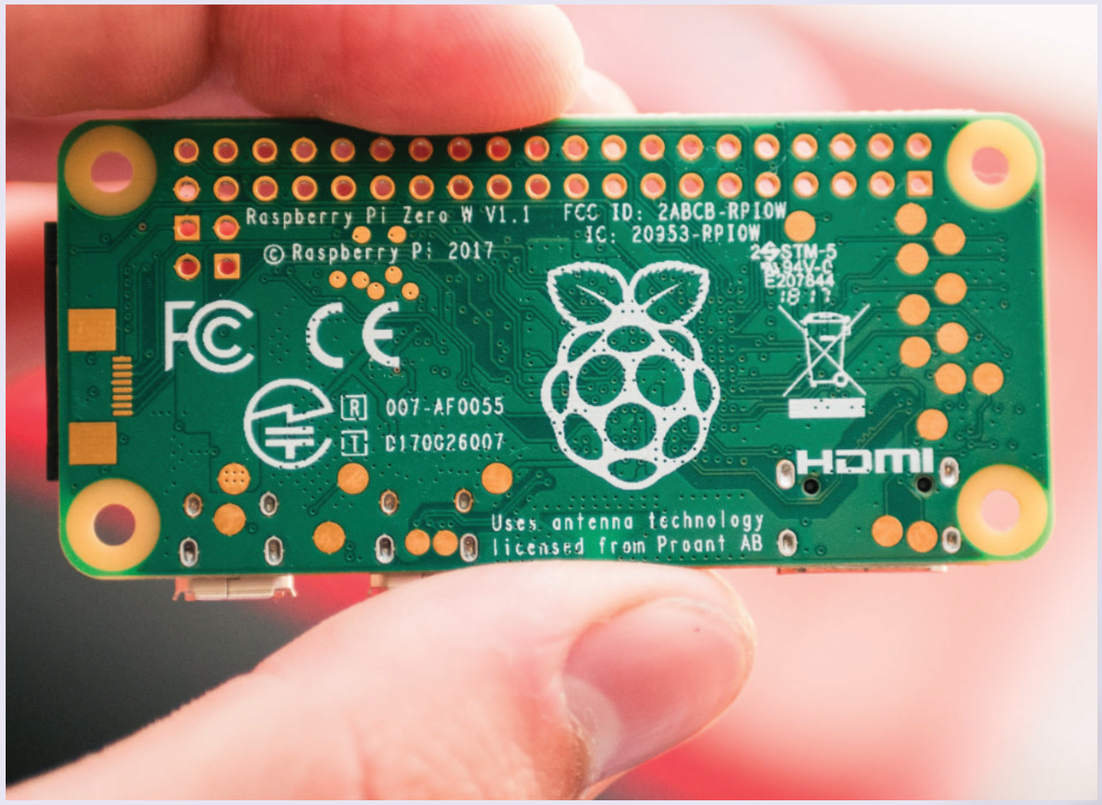
Un nœud Bitcoin Raspberry Pi vous ramène en arrière, à une époque où chaque objet de votre maison bremplissait une seule tâche précise: vous aviez une platine pour la musique, un téléviseur pour le divertissement audiovisuel et une console de jeux vidéo qui lisait des cartouches. Bien qu'il soit pratique de tout avoir sur un smartphone ou un ordinateur, il en résulte que ces appareils sont fondamentalement bien moins sûrs. C'est pourquoi il est important de disposer d'un matériel spécifique qui ne remplit qu'une seule tâche, surtout lorsque l'on parle d'argent (et d'argent sain qui plus est).

Cependant, Le Raspberry Pi 4 N'est PAS Un Matériel Open Source

Souvenez-vous quand dans le deuxième paragraphe je précisais que je ne suis pas rémunéré par la Fondation Raspberry Pi et que cet article représente uniquement le fruit de mes considérations? Et bien, je disais la vérité. Le Raspberry Pi est formidable dans ce qu'il fait, mais il subsiste pourtant quelques raisons pour lesquelles ce matériel n'est pas complètement idéal, ni en accord avec les valeurs fondamentales de Bitcoin.

Bitcoin c'est un code en open source, libre d'accès, que tout le monde peut lire, télécharger, vérifier et potentiellement modifier. Il fonctionne sur la base d'une philosophie permissionless dans laquelle il n'est pas nécessaire de faire appel à une quelconque autorité pour accéder au réseau. Les logiciels libres nécessitent également du matériel libre. Or, il n'y en a malheureusement pas assez à l'heure actuelle.

Pour être clair, si vous envisagez de construire votre propre Raspberry Pi parce que vous vous trouvez dans un pays qui vous empêche d'en importer un, ce ne sera pas chose aisée. De même, si vous devez remplacer ou améliorer certaines parties de la carte, il est également peu probable que vous puissiez trouver des pièces de rechange (à moins d'acheter un nouveau Raspberry Pi



complet). Cela fait partie du compromis qu'implique l'architecture des ARMs : on à affaire à des systèmes sur puce (SoC) et systèmes on modules (SoM) qui sont difficiles à répliquer si on souhaite utiliser les pièces "polyvalentes" qu'on peut trouver sur le marché.

On pourrait également débattre du fait que les puces sont potentiellement équipées de backdoor par la NSA: en tant qu'ordinateurs grand public, les Raspberry Pis sont très probablement surveillés et, c'est envisageable, piratables par les agences gouvernementales.

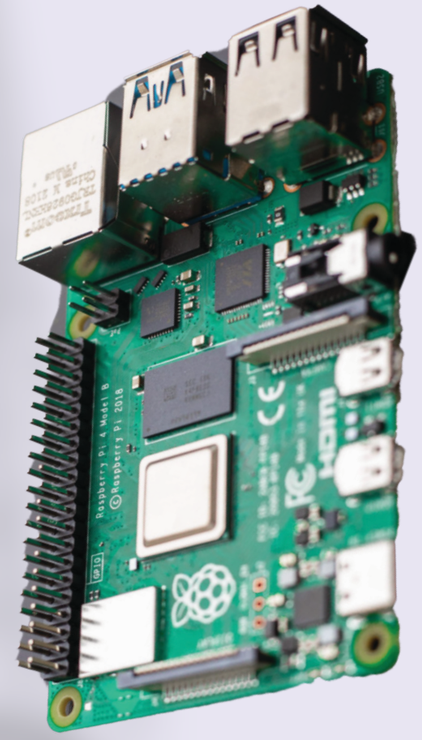
Si vous êtes vraiment à la recherche d'une expérience avec du materiel open source, orientez-vous plutôt vers les les ordinateurs RISC-V. En fabriquant ou bien en achetant (et en le vérifiant par la suite) l'un d'entre eux, vous savez que vous utilisez un open standard et que personne ne pourra compromettre votre appareil sans laisser de trace visible.

Il y a cependant une contrepartie pour ce surcroît de vie privée et il s'agit du prix: cet ordinateur qui permet à peine de surfer sur internet vous coûtera environ 3500 euros et le nombre de logiciels Bitcoin qui peuvent tourner dessus est bien plus limité.

Bien que Bitcoin Core tourne sur RISC-V depuis la sortie de la version 0.18.0 en mai 2019, je n'ai toujours pas trouvé de clients Lightning qui fonctionnent avec ces processeurs open source. Et si LND ou c-lightning ne fonctionnent pas, alors vous ne bénéficierez pas non plus des autres applications (RTL, LNBits, BTCPay et Sphinx Relay).

Une des raisons pour laquelle le standard RISC-V ne reçoit pas beaucoup de soutien est entre autre le coût du matériel – très peu de gens peuvent se l'offrir, ce qui est l'exact opposé de la raison pour laquelle le Raspberry Pi est si populaire.

Mais étant donné la récente résurgence du matériel open source grâce au Tropic Square de Trezor ou au projet Precursor de bunnie par exemple, on peut espérer qu'à l'avenir, une plus grande attention sera portée sur des processing units, de la mémoire RAM et des cartes mères qui seront véritablement open source et ne coûteront pas plus cher qu'un PC de gaming moyen.



Cela fait seulement 12 ans que Bitcoin a été lancé et 8 ans qu'Edward Snowden nous a révélé l'ampleur des opérations de surveillance de la NSA.

On peut ajouter que ce n'est qu'en 2018-2019 que le RISC-V est vraiment devenu populaire et que les fabricants de puces open source ont commencé vraiment à lever des fonds.

Il est certain qu'à l'heure actuelle, les ordinateurs de faible puissance comme le Raspberry Pi et l'Arduino règnent sur le marché, mais à l'avenir, nous pourrions très bien avoir du matériel entièrement open source permettant de faire tourner tous les excellents logiciels libres et open source Bitcoin.



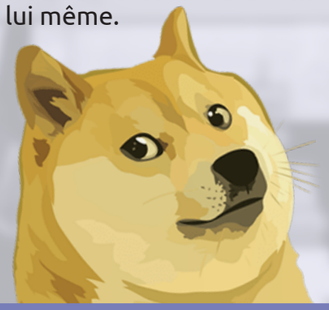


Elon Musk Ne Saisit Pas Ce Qu'est La Décentralisation, Mais Vous, Vous Devriez

La décentralisation est un concept difficile à apréhender et manifestement Elon Musk ne le comprend pas. Non seulement il a une vision puérile de la mise à l'échelle des blockchains et choisit de ne pas tenir compte des recherches existantes sur le sujet, mais il fait preuve d'une ignorance flagrante en ce qui concerne la concentration des ressources (un autre facteur qui rend un projet décentralisé) et ne semble pas saisir les incitations impliquées par un système basé sur la preuve de travail. En un mot, il est l'exemple parfait du meme "Je viens juste d'entendre parler de Bitcoin et je suis là pour le rectifier" (I just heard about Bitcoin – I'm here to fix it).

Peut-être qu'on ne devrait pas trop attendre d'un PDG passé maitre dans l'art d'obtenir des subventions gouvernementales tout en les critiquant et qui a par le passé participé à la création de PayPal, un moyen de paiement sur internet centralisé qui utilise l'argent hyper inflationniste des états, en s'appuyant sur un système qui génère des bénéfices même s'il cesse de facturer des frais de transaction (truquer les taux de change et collecter les données des utilisateurs est déjà bien suffisant).

Mais c'est pas parce que l'homme le plus riche du monde ne comprend pas Bitcoin (ou son fork meme-esque de prédilection, le Dogecoin) que vous ne devriez pas le comprendre non plus. En fait, je vais faire en sorte qu'au moment où vous aurez fini de lire cet article, vous saisirez ce que sont la décentralisation et Bitcoin bien mieux qu'Elon Musk lui même.



La Décentralisation Signifie Que Tout Le Monde Doit Être En Mesure De Participer Au Réseau

Le 16 mai 2021, Elon Musk a tweeté : "Idéalement, si Doge réduit le block time X10, augmente la taille des blocs X10 et diminue les frais X100. Alors il sera vainqueur haut la main".



Avant de commencer à analyser les implications plus profondes de ce tweet, je dois commencer par dire que le Bitcoin et le Dogecoin ont une architecture assez similaire en vérité. Après tout, le Dogecoin n'est qu'une copie de Litecoin en plus inflationniste (qui est déjà lui même un fork de Bitcoin ayant subit quelques légères modifications). Ainsi, même si certains paramètres tels que la taille des blocs, le block time (temps nécessaire pour produire un nouveau bloc) et l'offre totale sont différents d'une monnaie à l'autre, les principes sous-jacents sont exactement les mêmes – en particulier si l'on se concentre sur l'aspect de la décentralisation.

Mais revenons sur le tweet d'Elon Musk qui évoque 3 paramètres intrinsèques aux crypto-monnaies: le block time, la taille des blocs et les frais de transaction. Les deux premiers paramètres sont primordiaux pour établir la décentralisation, tandis que le troisième critère est lui essentiel pour assurer sa sécurité et sa pérennité sur la durée (et donc, là aussi sa décentralisation par effet de ricochet).

Le block time est le critère déterminant ceux qui auront la possibilité de valider la blockchain en fonction de la rapidité de leur accès à Internet. Le plus connu de tous, celui du réseau Bitcoin, est de 10 minutes, ce qui signifie qu'un nouveau bloc est miné environ toutes les 10 minutes.

Ça signifie que des nœuds du monde entier peuvent se synchroniser s'ils sont capables de télécharger 1 à 2 mégaoctets toutes les 10 minutes. C'est particulièrement intéressant lorsque les utilisateurs viennent de pays autoritaires où l'accès à l'internet est limité ou restreint. C'est également une excellente solution pour les personnes vivant dans les zones rurales des pays moins développés et qui n'ont pas toujours forcément accès à des connexions haut débit. N'importe qui dans le monde peut valider les blocs qui sont générés sur le réseau Bitcoin. Et théoriquement, les mineurs pourraient même effectuer leurs opérations au milieu d'un désert en se connectant au signal des satellites de Blockstream.

Déjà, le Dogecoin a un block time d'une minute – et ce modèle favorise les utilisateurs qui possèdent un accès internet très haut débit et la vitesse de connexion la plus rapide. Des milliards de personnes se voient ainsi refuser la possibilité de synchroniser leurs nœuds, parce que seuls les habitants des grandes métropoles sont en mesure d'obtenir toutes les données en temps réel. Ce paramètre est également inadapté pour la transmission interplanétaire (une des ambitions de Musk), car l'envoi d'un signal radio depuis la Terre vers Mars pourrait prendre entre 4 et 21 minutes (en fonction de la distance du moment). Bitcoin serait donc bien mieux adapté à un tel cas d'utilisation fantasmé.

Et pourtant, le block time de Dogecoin est loin d'être irraisonnable compte tenu de la demande étonnamment faible de block space. En fait, ce projet de 30 milliards de dollars ne traite qu'une poignée de transactions par bloc – ce qui est un assez bon indicateur de sa nature centralisée et

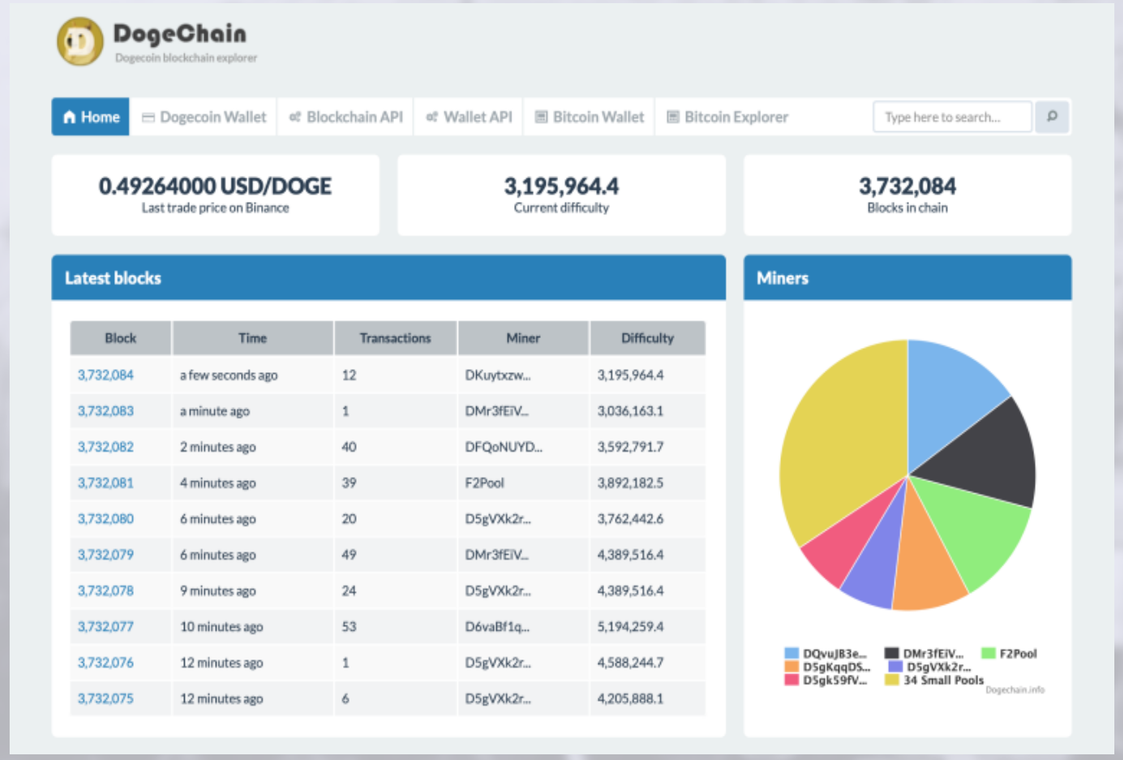
que la très grande majorité des transaction entre les particuliers est à mettre à l'actif des exchanges. La quantité de blocs vides sur le réseau Dogecoin en plein milieu d'un bull market (et d'une bulle spéculative évidente) est stupéfiante – il faut garder à l'esprit qu'une seule transaction par bloc signifie que l'envoi de la récompense au mineur qui a trouvé ce bloc correspond à cette unique transaction.

Cela nous amène à la partie concernant la multiplication par 10 de la taille des blocs de Dogecoin. Bien que ça paraisse complètement inutile compte tenu des données empiriques actuelles, supposons que d'une manière ou d'une autre les utilisateurs commencent à utiliser cette blockchain. Si les transactions Dogecoin remplissaient des blocs de 10 mégaoctets toutes les 6 secondes, alors le ledger publique augmenterait de 100 mégaoctets par minute, soit 6 gigaoctets par heure, 144 gigaoctets par jour et donc 4,32 téraoctets par mois. C'est quasiment aussi aberrant que sur Chia, l'effroyable et pourtant survendu projet Frankenstein de la preuve de travail de Bram Cohen.

Bien sûr, ce scénario est assez peu probable, puisque même dans le cas de Bitcoin, il arrive régulièrement que les blocs ne soient pas complètement pleins. Mais même si un quart de l'espace de bloc est rempli en moyenne, la blockchain Dogecoin augmentera de 252 gigaoctets par semaine. A titre de comparaison, il aura fallu 12 ans à la blockchain Bitcoin pour atteindre une taille de 350 gigaoctets.

Pour une majorité de gens dans le monde, un disque dur de 1 téraoctets c'est plutôt cher. Mais si Dogecoin émettait des blocs de 10 mégaoctets chaque minute, alors un disque dur de 1 To serait remplie au bout d'une semaine. En contraste, la blockchain Bitcoin ajoute environ uniquement 51 gigaoctets de données par an, de sorte que le même disque dur de 1 To devrait être suffisant pour environ 19 années supplémentaires de fonctionnement d'un nœud d'archivage complet.

Lors de la conception d'un système décentralisé, on doit s'assurer de n'exclure personne pour des raisons financières avec des mises à jours discriminatoires du réseau. Si on ne peut pas valider ses propres





transactions et vérifier l'état de l'ensemble du réseau à l'aide de son propre nœud, alors le système est centralisé.

Internet n'exige pas d'avoir un ordinateur haut de gamme pour accéder aux pages web – et en tant que système monétaire, Bitcoin vise à être aussi inclusif et ouvert au plus grand nombre de personnes sur cette planète. Elon Musk ne comprend manifestement pas ça et cherche à centraliser un projet abandonné mais "meme-able" sous sa propre gentille dictature imprévisible, et souhaiterait transformer un projet universel et ouvert en un petit jouet personnel.

Pour résumer : si vous ne pouvez pas rejoindre le réseau en tant que nœud de validation, alors le projet n'est pas décentralisé. Diminuer l'intervalle de temps entre les blocs exclut les personnes ayant des connexions Internet lentes, tandis qu'augmenter la taille des blocs augmente les coûts de stockage et de calcul de tous les participants (éliminant de fait ceux qui ne se mettent pas à jour régulièrement). C'est pour cette raison que des solutions de secondes couches telles que le Lightning Network existent. Mais apparemment ce que souhaite Elon Musk c'est produire un nouveau Paypal.

La Décentralisation Nécessite Des Incitations (Cela Inclue Les Frais De Minage)

Bien que le Dogecoin soit pour le moment extrêmement inflationniste, les récompenses de minage vont être considérablement diminuées au cours des années à venir en raison des halvings programmés. Il en va de même pour Bitcoin qui renforce un peu plus son jeu de raréfaction grâce au mécanisme déflationniste activé tous les 210 000 blocs (environ tous les 4 ans).

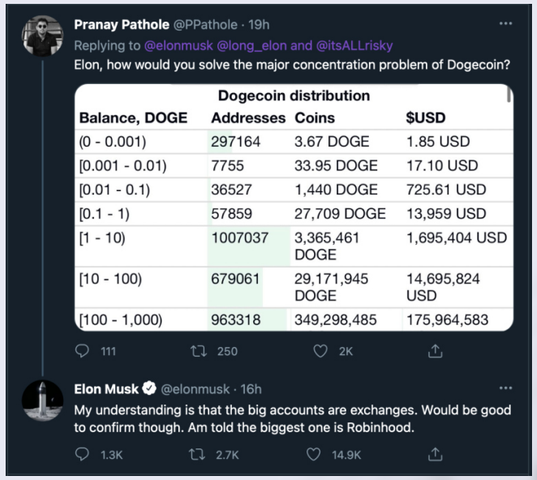
À mesure que la récompense pour la découverte d'un bloc diminue, les mineurs devraient être incités à continuer à sécuriser le réseau. À la quatrième page de son white paper par lequel tout à commencé, Satoshi Nakamoto décrit un système qui finit par ne plus subir d'inflation et dont les mineurs sont incités à poursuivre leurs activités grâce aux frais de transaction.

Sans ces frais, le système d'incitation cessera d'exister et il est probable que de nombreux mineurs arrêteront de soutenir le réseau. Toutefois, la réduction des frais de 100X décrite par Elon Musk pourrait s'avérer être la solution idéale qui lui permettrait de prendre le contrôle du réseau en continuant à extraire des blocs à perte mais en maintenant de fait son emprise.

Diminuer arbitrairement les frais aurait pour conséquence de réduire le nombre de mineurs. Et moins de mineurs signifie moins de décentralisation et donc plus de chances de contrôler le réseau. Même si c'est peut-être ce que recherche Elon Musk, c'est une idée épouvantable. Il n'y a rien de révolutionnaire ou de disruptif dans un système où l'homme le plus riche du monde peut jouer les censeurs – après tout, c'est la dynamique de la géopolitique qui rend Bitcoin ou Dogecoin plus fongibles et résistants au "blacklistage" potentiel des transactions.

Payer 100 fois moins de frais semble une idée formidable sur le papier, mais sur le long terme, cela ne ferait qu'éroder le système et conduirait à un contrôle/centralisation accru

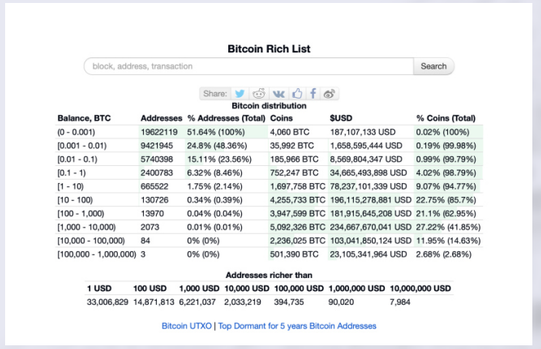
et à plus d'inflation. En plus de ça, les frais représentent un mécanisme efficace pour empêcher les spams par transactions – s'il y a un coût, les gens sont moins susceptibles d'encombrer le réseau avec un nombre élevé de petites transactions parce qu'ils doivent payer pour chacune d'elles. La vision de Musk pour Dogecoin est clairement incorrecte sur le plan technique.



Décentralisation Et Répartition Des Richesses

Le 17 mai 2021, Elon Musk a répondu aux inquiétudes de Pranay Pathole au sujet de la concentration de richesse sur Dogecoin. Selon Bitinfocharts, 107 adresses Dogecoin possèdent plus de 66,7 % de l'offre. En outre, une adresse possède à elle seule 28,34 % de l'ensemble de l'offre – un montant disproportionné, compte tenu des ambitions supposées du projet. Elon Musk a choisis de ne pas se pencher de manière nuancée sur la question, et a proposé une réponse générique en émettant l'hypothèse que Robinhood pourrait potentiellement être la plus grosse whale (gros détenteur du coin). Bien que cette affirmation puisse potentiellement être possible, il n'existe a aucune confirmation allant dans ce sens.

Mais comparons cette situation à celle de Bitcoin. Les trois adresses les plus fournies sont clairement identifiées comme étant celles des fonds conservés en cold storage par Huobi, Binance et Bitfinex. Et en cumulé, elles possèdent au total 2,68% des fonds totaux du réseau – c'est un fait clairement établi, ces plus grosses adresses représentent en réalité les réserves de centaines de milliers de clients.



Sur Bitcoin, il y a actuellement environ 16 000 adresses qui possèdent 62,95 % de l'offre. Ce n'est clairement pas idéal, mais c'est toujours mieux que la situation de Dogecoin, où 107 adresses détiennent plus d'un tiers des unités de cette monnaie. La situation sur Ethereum est encore pire, avec des portefeuilles individuels détenant des quantités énormes de coins (très probablement une conséquence de leur premine de 60 % et du fait que certains des premiers investisseurs ou cofondateurs n'ont jamais vendu).

Mais pourquoi la répartition des richesses est-elle si importante pour la décentralisation? C'est aussi une question d'incitations et d'inclusion. Personne ne voudrait prendre part à un projet où un petit nombre constituant une sorte d'élite contrôlerait la majeure partie de l'argent. Les investisseurs ne voudraient pas être soumis à un tel risque, les développeurs ne voudraient pas être sous le contrôle de ces quelques acteurs, et les mineurs considéreraient également cette centralisation contrariante et pas viable sur long terme.

Ces gros détenteurs sont de potentiels point unique de défaillance qui faussent le jeu pour tous les autres autour. La détention de grosses réserves peut également potentiellement signifier une plus grande influence sur le développement du projet et un certain pouvoir politique sur le réseau. Ce qui est clairement une menace pour un réseau non entretenu comme celui de Dogecoin.

Ne Le Dites Pas À Elon Mais Dogecoin Est Une Chaîne Au Hashrate Minoritaire Qui Est Minée En Simultané Avec Litecoin

La continuation de l'existence de Dogecoin en tant que réseau est due uniquement à une pure bienveillance de la part de certains intervenants. Pour être plus clair, les mineurs de Litecoin ont décidé de sauver le Dogecoin en 2014 en lui permettant d'être miné en simultané (merge mining). Ainsi, au lieu de devenir vulnérable aux attaquants malveillants, le réseau est protégé par certains des mêmes mineurs Scrypt qui sécurisent la chaîne au hashrate majoritaire.

Le minage Litecoin est presque aussi énergivore que celui de Bitcoin, mais il diffère à certains égards au niveau des spécifications techniques (le SHA 256 de Bitcoin est gourmand en terme de processeur, tandis que le Scrypt de Litecoin et Dogecoin est plutôt gourmand en terme de mémoire).

Mais si Elon Musk décide de critiquer le minage de Bitcoin tout en continuant de fermer les yeux sur la façon dont le Dogecoin est produit, il n'est alors qu'un hypocrite qui envoie des signaux de vertu avec des données soigneusement sélectionnées pour s'attirer la bienveillance d'une foule de gens mécontents (et "éveillés") tout en protégeant ses transactions en Dogecoin sous un voile d'ignorance.



Le moins que l'on puisse dire, c'est qu'Elon Musk est malhonnête intellectuellement, incohérent et fortement biaisé. S'il était laissé à lui-même, le Dogecoin deviendrait la proie d'attaquants qui peuvent se permettre de louer quelques machines de minage pour quelques heures. Et si le projet venait à être coopté par Tesla ou SpaceX, alors il perdrait sa proposition de valeur.

Les Changements Proposés Par Elon Musk Nécessitent Un Hard Fork Centralisé

Les hard forks sont des modifications du réseau impliquant la migration de l'ensemble des participants sur la nouvelle blockchain. Une incompatibilité entre l'ancienne et le nouvelle blockchain en résulte, et par conséquent tout repose sur le consensus selon lequel tout le monde doit rejoindre la nouvelle chaîne.

Plus il est facile de réaliser un hard fork, plus le projet est centralisé. Idéalement, les opérateurs de nœuds et les mineurs souverains devraient être sensibles aux nouveaux changements, rejeter le leadership et choisir de vérifier chaque ligne du code de manière individuelle et avec ses propres intérêts à l'esprit. Mais quand l'homme le plus riche du monde se présente et dit qu'il veut assumer un rôle de leader, c'est déjà un mauvais signe qui conduira sans aucuns doutes à plus de centralisation. Et oui, pour être clair, je suis également critique de l'implication de Michael Saylor dans Bitcoin.

Les exchanges vont-ils soutenir un hard fork juste parce qu'Elon Musk est impliqué dedans? On peut raisonnablement en douter, car beaucoup d'entre eux ont des principes et essaient vraiment d'analyser les fondamentaux sur le long terme (contrairement à des casinos comme Binance, qui semble soutenir tout ce qui peut générer un volume de transactions).

Les utilisateurs migreront-ils vers le Dogecoin Elon's Vision (DEV) ? Eh bien, il n'y a pas tant d'utilisateurs que ça au sens où on l'entend pour Bitcoin (des nœuds souverains). Il reviendra donc aux exchanges et aux entités qui ont un intérêt à faire

tourner un noeud de prendre leur décision. Cependant, il y a une bien trop grande part de centralisation dans tout ça.

A titre de référence, les développeurs Bitcoin font le maximum pour éviter les hard forks. Le récent "trial" pour Taproot a prouvé définitivement que le réseau est suffisamment mature pour décider de manière décentralisée d'un soft fork (une mise à jour qui ne modifie pas les règles de consensus et qui reste facultative pour l'ensemble du réseau).

Il Y A Une Raison Pour Laquelle Le Développement De Bitcoin Est Aussi Prudent: La Décentralisation Ça Marche

La décentralisation c'est compliqué à établir. Si vous êtes un nouveau-venu dans ce milieu et que vous êtes habitué à un univers où les mises à jour des applications sur votre téléphone sont déployées et installées en quelques minutes seulement, vous aurez du mal à comprendre un système comme Bitcoin qui repose sur de longues délibérations et a tendance à s'ossifier (devenir de plus en plus rigide) au fil du temps.

Si améliorer une blockchain était aussi trivial, Bitcoin n'aurait-il pas d'ailleurs lui aussi déjà de plus gros blocs, des block times plus rapides et des frais moins élevés? C'est vraiment naïf de penser que ces propositions sont inédite et que personne n'a jamais pensé à les mettre en pratique avant.

Et la mentalité de la Silicon Valley, qui consiste à aller vite quitte à casser des choses au passage (move fast and break things), n'est certainement pas adaptée à un système monétaire qui est censé sécuriser l'épargne de chacun plutôt que de la rendre rapide et facile à transférer.

Le Dogecoin n'était pas censé atteindre une capitalisation aussi élevée et n'a certainement pas été créé dans le but d'accroître la richesse et l'influence de l'homme le plus riche du monde.

Mais voilà où on en est... On en est réduits à éclaircir ce sujet et à tenter de définir à quoi la décentralisation devrait ressembler – et répondre de manière frontale aux élucubrations mal informées d'Elon Musk.

La décentralisation c'est difficile – et j'espère que ce long article de ma part vous aura aidé à la comprendre mieux qu'Elon Musk.







Les NFTs Bitcoin Sur Counterparty (Et Comment Obtenir Ou Créer Votre Premier NFT)

Omniprésents sur l'ensemble des médias et pourtant largement incompris, les NFT sont les sujets de fascination et (surtout) de spéculation irrationnelle de ce cycle. En raison du battage excessif associé à ce mouvement "looks rare", certains observateurs sont allés jusqu'à comparer, et à juste titre d'ailleurs, les NFTs aux ICOs de 2017 et 2018. Cette exubérance pour les actifs rares et la facilité à "minter" (émettre) les NFTs ont conduit à une situation où tout le monde semble émettre et vendre tout ce qui peut s'apparenter de près ou de loin à une pièce de collection.

Mais contrairement aux ICOs, avec les NFTs, ce que vous voyez, c'est ce que vous avez. Personne n'achète ces jetons en espérant autre chose que de recevoir un actif numérique unique associé à une œuvre d'art. Quand les ICOs étaient accompagnées de feuilles de route et de promesses sur l'avenir du projet, les NFTs sont simplement des hashs cryptographiques écrits sur la blockchain. En gros, il s'agit de cartes de baseball à collectionner pour les nerds.

Il convient également de mentionner que tous les NFTs ne sont pas créés égaux : si les jetons ERC-721 sur Ethereum sont les plus connus et les plus commercialisés, il existe également des jetons de la sidechain Liquid qui sont échangés sur Raretoshi par exemple. Toutefois, les jetons vraiment spéciaux sont émis sur la blockchain Bitcoin via Counterparty.

Ils bénéficient du réseau le plus sécurisé de tous, ils sont stockés sur pratiquement tous les nœuds souverains et reçoivent des noms uniques qui agissent un peu comme comme des domaines Internet ne pouvant être reproduits. Si on considère que le jeton représente l'oeuvre, alors ce sera le plus résistant et celui avec la preuve la plus infalsifiable de son unicité qui aura le plus de chances de résister à l'épreuve du temps.



Et oui, il y a bien aussi l'oeuvre qui y est associé. Présenté sous la forme d'un jpeg, d'un gif, d'un lien YouTube ou même d'un fichier audio, il s'agit en gros de la représentation visuelle mutable et modifiable du jeton. Mais le fichier "artistique" lui-même n'est pas stocké sur la blockchain: la plupart de ces fichiers n'existent que sur Imgur, IPFS ou autre sites Web centralisés et spécialisés dans le téléchargement et le partage d'images. Ça implique qu'il ne faut pas considérer le jpeg autrement que comme un bel emballage offrant des détails visuels sur ce qui se cache derrière le jeton.

Bien que certains utilisateurs intentent des procès et s'offusquent quand la même image est utilisée pour émettre un autre NFT, ils ne doivent pas oublier qu'ils ont en fait payé pour un jeton unique qui ne peut pas être reproduit. Il est "non fongible" (vous ne pouvez pas le remplacer par un autre, car il n'existe pas de hachage identique) et c'est essentiellement ce que Hal Finney a décrit en 1993 en suggérant comment les cypherpunks peuvent avoir "des heures de fun" avec ça.

Crypto trading cards.

- *To*: CYPHERPUNKS <CYPHERPUNKS@TOAD.COM>
- *Subject*: Crypto trading cards.
- *From*: Hal <74076.1041@CompuServe.COM>
- *Date*: 17 Jan 93 13:48:02 EST

Giving a little more thought to the idea of buying and selling digital cash, I thought of a way to present it. We're buying and selling "cryptographic trading cards". Fans of cryptography will love these fascinating examples of the cryptographic arts. Notice the fine way the bit patterns fit together - a mix of one-way functions and digital signatures, along with random blinding. What a perfect conversation piece to be treasured and shown to your friends and family.

Plus, your friends will undoubtedly love these cryptographic trading cards just as much. They'll be eager to trade for them. Collect a whole set! They come in all kinds of varieties, from the common 1's, to the rarer 50's, all the way up to the seldom-seen 1000's. Hours of fun can be had for all.

Your friendly cryptographic trading card dealer wants to join the fun, too. He'll be as interested in buying your trading cards back as in selling them.

Try this fascinating and timely new hobby today!

Hal

Comme on a établi précédemment, les images ne sont que des représentations visuelles qui vous aident à comprendre ce dont il est question derrière le jeton. Cependant, c'est cet oeuvre totalement fongible et reproductible qui attire initialement votre attention et vous donne envie de soutenir le travail d'un certain artiste. Certains de ces fichiers (le plus souvent des jpegs et des gifs) ont le mérite d'être artistiques, d'autres ont un côté amateur, mais la plupart d'entre eux ont en fait l'air baclés, peu inspirés, et n'existent probablement que pour gagner un peu d'argent en profitant de l'effet de mode.

C'est pourquoi j'ai tendance à être pessimiste concernant les NFTs sur Ethereum et Solana, mais au contraire optimiste en ce qui concerne les créations Bitcoin sur Counterparty : les oeuvres ne sont pas seulement meilleures, mais aussi suffisamment intemporelles pour pouvoir résister à l'épreuve du temps et faire un retour en force même après l'explosion inévitable de la bulle actuelle. Les bitcoiners construisent des protocoles et des couches qui durent et trouvent une utilité souvent des années après qu'ils aient été déclarés morts et abandonnés. Du côté d'Ethereum, il s'agit par opposition de constamment trouver de nouvelles sources de hype et d'enterrer de manière opportune chacun des échecs passés. En 2021, la couche Omni a été ravivée par le projet Synonym de John Calvalho, tandis que Counterparty a de nouveau été mis en avant en s'appuyant sur sa riche histoire artistique. Aucunes chances de lire des news similaires concernant Raiden ou Plasma.





D'où Viennent Les NFT ?

Il s'agit de bien plus que ces jpegs qui focalisent l'attention. Comme tout ce qu'Ethereum a touché et transformé en fosse aux lions sans âme, financée par des VC et non scalable, les NFTs ont d'abord été popularisés par le protocole Counterparty de Bitcoin entre 2014 et 2016.

Il faut savoir que c'est Namecoin (anciennement connu sous le nom de BitDNS, un hard fork de Bitcoin que Satoshi Nakamoto lui-même a adoubé) qui a été crédité pour l'émission des premiers NFTs de l'histoire : Quantum, Blockheads, Comicons et Cryptoeggs étaient essentiellement des projets d'avatars visant à fournir à chaque nouvel utilisateur une identité numérique unique. Ils n'étaient pas destinés à devenir des objets de collection, mais les gens ont commencé à se les échanger et ils ont pris de la valeur sur le marché. Plusieurs années plus tard, Ethereum a copié cette approche avec ses CryptoPunks et d'autres avatars similaires générés numériquement que vous pouvez apercevoir aujourd'hui sur certains avatars Twitter.

Mais après le lancement du protocole Counterparty en janvier 2014, les bitcoiners ont commencé à créer leur propre forme d'art tokenisé. À partir de ce moment-là, on peut identifier deux écoles de pensée importantes: d'un côté celui de l'innovation en matière d'actifs de jeux vidéo (les cartes "Spells of Genesis" de Shaban Shaame et "SaruTobi Island" de Christian Moss étant deux des meilleurs exemples) et de l'autre celui des mèmes (Rare Pepes, Fake Rares, Leftist Tears, Bitcoin Heads).

Bien sûr, tous ces NFTs ne sont pas apparus en 2014. Le directory Rare Pepe a été créé en septembre 2016, les cartes Spells of Genesis sont apparues pour la première fois en septembre 2015, tandis que les Fake Rares et les Bitcoin Heads ont été émis durant la seconde moitié de 2021.

Pourtant, l'élément qui les fait se démarquer c'est qu'ils sont générés par les utilisateurs au moyen de logiciels de



conception graphique ou même de dessins à la main. Les bitcoiners adorent les preuves de travail – donc, contrairement à leurs homologues sur Namecoin ou Ethereum, ils n'émettent pas d'œuvres d'art générées automatiquement par un ordinateur. Vous pouvez retrouver cette charmante patte humaine dans toutes ces NFTs Bitcoin.

Pour en savoir plus sur l'histoire des NFTs, vous pouvez lire l'excellent article de WhiteRabbit1111 intitulé "The origin assets of the digital antiquities market (NFTs)". Il s'agit d'une plongée en profondeur dans toutes sortes de projets, dont certains sont moins connus mais méritent des éloges pour avoir été les pionniers de ce qui se transformera plus tard en une industrie pesant plusieurs milliers de BTC.

C'est Quoi Counterparty ?

Counterparty est un protocole Bitcoin rarement mentionné dans les livres d'histoire. Même "Mastering Bitcoin", sans doute la publication la plus complète et la plus exhaustive sur le sujet, ne décrit Counterparty que rapidement dans un seul paragraphe avant de passer aux altcoins (qui bénéficient eux d'une plus grande couverture).

On pourrait penser que Counterparty n'est qu'une relique d'un passé longtemps oublié; une ville fantôme qui nous rappelle les premières intentions et aspirations des bitcoiners. Il s'agit pourtant en fait simplement d'un protocole qui permet toujours aujourd'hui à quiconque d'émettre des jetons sans autorisation et de mettre en place des contrats qui verseront des dividendes aux détenteurs de ces jetons. Counterparty est un prototype authentique de ce qui allait par la suite devenir le projet Ethereum, à ceci près qu'il a été lancé de manière équitable, qu'il ne dispose pas de sa propre blockchain et que toutes ses transactions (depuis l'émission jusqu'aux transferts) sont réglées sur la blockchain Bitcoin et que les frais de transaction sont versés aux mineurs Bitcoin.



Les NFTs de Counterparty représentent souvent des moments clés de l'histoire de Bitcoin.

En 2014, les bitcoiners rêvaient de tokeniser les actions et les matières premières sur leur réseau de prédilection. Échanger des actions Apple, des contrats à terme sur les fèves de cacao et des lingots d'or sur Bitcoin? Bien sûr, pourquoi pas! Créer des entreprises décentralisées dont les actifs existent nativement sur le réseau Bitcoin? C'est également possible avec Counterparty. Des jetons destiné aux collectes de fonds et qui versent des dividendes à leurs propriétaires? Oui, monsieur !

Mais ça c'était avant le débat sur la mise à l'échelle et avant de décider que les blocs devaient rester petits pour préserver la décentralisation et la résistance à la censure. La plupart des personnes à l'origine du projet sont ensuite passées sur le tout nouveau et tout brillant Ethereum, qui pouvait techniquement faire plus et théoriquement mieux s'adapter à ces cas d'utilisation.

En effet, pendant un certain temps, les transactions de Counterparty ont été injustement considérées comme du "spam" qui allait à l'encontre des intérêts du projet Bitcoin. On pourrait certes arguer que le transfert d'argent d'une personne lambda peut potentiellement être confirmé moins rapidement en raison d'échanges intensifs de jetons Counterparty, puisque le premier paie des frais moins élevés que le second. De plus, les transactions OP_RETURN que Counterparty utilise pour insérer des données arbitraires dans les blocs Bitcoin prennent plus d'espace de bloc qu'une transaction ordinaire.

Mais là encore, ça signifie que les frais payés sont plus élevés. Et il est clair que si l'on souhaite que les incitations du projet Bitcoin soient durables, on doit créer un marché des frais compétitif. Il y a aussi un autre petit détail et c'est ceui qui affirme que le réseau Bitcoin est sans permission et permet aux utilisateurs d'être souverains (c'est-à-dire d'utiliser leur propre argent comme ils le souhaitent). Sous cet angle, comment un utilisateur de Counterparty peut-il être considéré comme un spammer s'il paie sa juste rémunération aux mineurs ?



Counterparty a clairement été du "mauvais" côté de l'histoire de Bitcoin et beaucoup ont choisi de ne pas en parler du tout. Il possède un jeton natif (XCP) qui est utilisé pour donner un nom arbitraire aux actifs : si vous payez 0,5 XCP, vous pouvez appeler votre nouveau NFT "BTCTKVRMAG" au lieu de laisser le protocole le nommer automatiquement "A1111376119 1968729490" (où "A" signifie "actif"). Vous pouvez également vendre vos nouveaux jetons et donner des dividendes aux détenteurs en utilisant le jeton XCP.

Mais il y a un hic : Counterparty a été créé par des bitcoiners qui ont assisté à l'ICO de Mastercoin (qui est devenue plus tard la couche Omni) et ils l'ont détesté. Les créateurs du protocole ne voulaient pas faire une collecte de fonds et offrir aux investisseurs des jetons en échange. Ce n'est pas assez "esprit Bitcoin".

Ils ont donc demandé aux participants de "brûler" leurs BTC et de recevoir des XCP en échange. Cela signifie qu'en janvier 2014, près de 2131 bitcoins ont été envoyés de manière irréversible à l'adresse 1CounterpartyXXXXXXXXXXXXXUWLpVr. Ils ont donc volontairement créé une adresse difficile à générer et à laquelle personne n'a accès. Ainsi, pour créer la totalité des 2 648 755 jetons XCP, de vrais BTC ont pour l'occasion été brûlés.

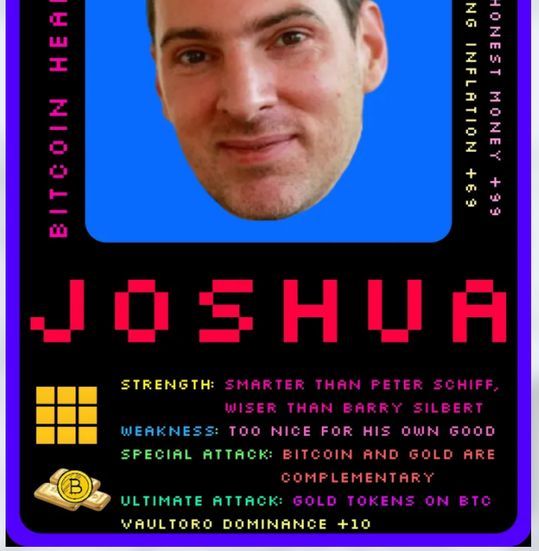
Selon l'article "Why Proof-of-Burn" du 23 mars 2014, les bitcoiners qui ont créé Counterparty ne voulaient pas que les développeurs jouissent d'un avantage injuste et ils ne voulaient pas non plus que les gros investisseurs aient un quelconque contrôle sur le réseau. Tout le monde avait une chance égale de brûler des BTC et de recevoir des XCP en échange. De plus, personne n'avait un avantage à être le premier arrivé, il n'y a donc pas d'entité centralisée pour coordonner un système de pump and dump. Chacun à autant d'intérêt à la réussite du projet et doit faire face aux mêmes risques.



Pourtant, ça ne signifie pas que la valeur du jeton XCP est liée au prix du BTC, ou que la capitalisation boursière devrait être équivalente aux 2131 BTC. A la date du 30 juin 2022, 2131 BTC valent 41 millions de dollars, alors que l'ensemble du supply de XCP ne vaut que 6,4 millions de dollars. Cette comparaison n'est d'ailleurs même pas nécessaire pour prouver que XCP est simplement un jeton utilitaire qui ne concurrence pas le bitcoin. Il n'est pas censé être une réserve de valeur; vous l'achetez uniquement pour émettre votre actif auquel vous attribuez un nom et afin de l'utiliser pour la fonction auquel il est destiné. Il serait insensé de détenir des XCP à des fins spéculatives, car le token n'est même pas côté sur les exchanges populaires et le seul moyen de l'acquérir est de passer par des dispensers (distributeurs).

En parlant de dispensers, Counterparty peut également être considére comme un véritable exchange décentralisé. Tout le monde peut vendre des actifs sans demander l'autorisation à qui que ce soit et faire en sorte que les BTC (ou tout autre jeton Counterparty)soient automatiquement envoyés dans un portefeuille personnel après le règlement de chaque transaction sur la chaîne principale.

Si vous souhaitez acheter 0,5 XCP avec votre BTC pour donner un nom à votre tout nouveau NFT ou bien émettre des dividendes aux détenteurs de vos NFTs déjà existants, alors rendez vous sur un dispenser et recherchez l'utilisateur qui propose l'offre la plus avantageuse. FreeWallet.io, probablement la meilleure interface Counterparty disponible à l'heure actuelle, vous permet de naviguer entre les exchanges (marchés ouverts pour les diverses paires de tokens) et les dispensers (distributeurs automatiques où vous achetez/vendez des token Counterparty et des NFTs contre des BTC).



L'aspect "vanité" de l'émission de jetons avec un nom qui leur est associé est assez unique à Counterparty. Si vous regardez les NFTs Raretoshi sur Liquid par exemple, vous remarquerez qu'ils portent un nom d3 hachage cryptographique aléatoire (par exemple, e9f53c1fd6f71eccbe2f3

bf5523ef29d1de9fbb9a155c7682808ffcd17299728). Sur Ethereum, ils portent le nom du contrat (par exemple, le spinoff PEPEGOAT de JScrilla Rare Pepe Wallet ReDux s'appelle 0xb932a70A57673d89f4acfFBE830E8ed7f75Fb9e0). La principale différence c'est que sur Counterparty, vous achetez des actifs portant un nom qui leur est propre et vous pouvez utiliser le nom du jeton pour rechercher tout type d'information sur ses transactions dans l'explorateur xchain.

Counterparty est en gros une version primitive d'Ethereum qui a été construite sur la blockchain Bitcoin en tant que protocole et dont les transactions sont réglées en BTC, tout en payant des frais aux mineurs Bitcoin. Il a très probablement été abandonné parce qu'il a de gros problèmes de scalabilité. Mais à l'été 2021, alors que la frénésie des NFT était à son apogée et qu'Ethereum devait faire face à des frais ridiculement élevés, les bitcoiners se sont souvenus de Counterparty et ont profité de la faible demande de block space sur Bitcoin pour redonner vie à des oeuvres anciennes.

Alors que certains déconseillent l'utilisation de Counterparty et recommandent Raretoshi sur la sidechain Liquid ou RGB Spectrum sur le Lightning Network, la réalité c'est qu'aucune de ces solutions n'est aussi sûre ou décentralisée que la blockchain Bitcoin. En plus, aucune d'entre elles n'offre la garantie de vivre aussi longtemps que la couche de base elle-même. Et comme il y a beaucoup de collections qui existent sur Bitcoin, il y aura toujours des collectionneurs pour s'y intéresser. L'objectif n'est clairement pas de "passer à l'échelle", mais d'assurer la sécurité et longévité les plus grandes aux actifs.

Comme Bitcoin, Counterparty a été déclaré "mort" à de nombreuses reprises auparavant, mais il a fait quelques retours notables, notamment parce qu'il est construit sur Bitcoin et nécessite une maintenance minimale – les actifs existeront toujours et ils sont sécurisés par un réseau mondial de mineurs et de nœuds, de sorte que seules les interfaces utilisateur (portefeuilles) ont besoin d'être améliorées de temps en temps. Vos NFTs peuvent certes coûter plus cher à créer et à transférer (par rapport aux plateformes centralisées comme Liquid ou Ethereum), mais ils sont aussi plus

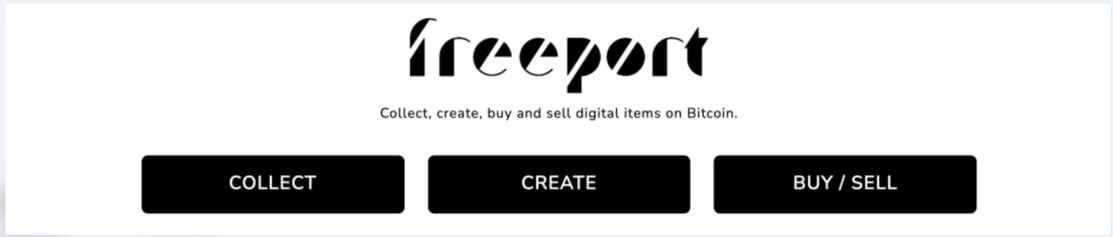


sûrs parce qu'il est pratiquement impossible de stopper le réseau. Et puis, est-ce que c'est vraiment de la shitcoinerie si vous construisez au-dessus de Bitcoin et contribuez au budget de sécurité du réseau en payant des frais pour chaque transaction?

Comment Créer Votre Premier NFT Bitcoin Sur Counterparty Avec Freeport

Selon l'importance que vous accordez au nom de votre actif, il y a deux façons d'émettre des NFTs Bitcoin sur Counterparty et elles se démarquent par des niveaux de difficulté différents. La méthode la plus simple, et de loin, est de se procurer le wallet FreePort de Joe Looney (disponible sous forme d'extension pour navigateur Chrome et Firefox), de transférer l'équivalent de quelques transactions en BTC, puis de suivre l'interface utilisateur simple pour télécharger votre jpg/gif et émettre votre NFT.

Si vous utilisez FreePort, vous n'aurez jamais à toucher à XCP et à vous compliquer la vie en l'achetant via des dispensers. Vous pourrez émettre, envoyer et admirer les NFT de votre collection à l'aide d'une interface très simple. Voici donc les étapes à suivre :



1. Allez sur https://github.com/loon3/Freeport-extension

2. Si vous utilisez Chrome, cliquez sur l'URL située sous "Install from Web Store" et suivez les instructions à l'écran. Une fois que vous aurez terminé, vous remarquerez le logo Freeport en haut à droite de votre fenêtre Chrome, juste à côté de la barre d'adresse et à gauche du menu des options.

3. Si vous utilisez Firefox, vous devez utiliser la ligne de commande web-ext pour installer le fichier disponible à l'adresse https://github.com/loon3/Freeport-extension/raw/dev/packages/freeport-0.3.0-fx.xpi. Cette méthode est plus compliquée et vous devrez lire la syntaxe telles que "web-ext run". Cependant, si vous souhaitez échapper au panopticon de Google, ça en vaut la peine.

4. Créez un nouveau portefeuille avec Freeport. Par défaut, il va générer un seed BIP39 de 12 mots et vous devez également configurer une passphrase (je recommande d'utiliser à la fois des lettres et des chiffres) pour déverrouiller vos actifs. Il s'agit en gros d'un portefeuille Bitcoin, alors traitez-le comme tel – prenez soin de votre seedphrase, ne la révélez jamais à quelqu'un d'autre et notez-la sur un morceau de papier ou gravez la sur du métal.

5. Une fois que vous êtes configuré et connecté, vous verrez le menu principal de Freeport qui comporte trois boutons : Collect, Create, et Buy/Sell. Dans le coin supérieur gauche, vous verrez votre adresse Bitcoin Counterparty, et dans le coin supérieur droit, vous trouverez un bouton orange qui affiche le logo Bitcoin – celui-ci vous permet de vérifier votre solde BTC et d'envoyer des montants arbitraires. Remarquez également que dans le menu du bas, vous avez un bouton "Settings". Vous pouvez l'utiliser pour modifier votre adresse de réception/émission de NFT (une fonctionnalité que vous ne trouverez jamais sur Ethereum car il n'a pas d'UTXO par conception), afficher votre passphrase (ne faites jamais de captures d'écran), définir manuellement les frais de transaction et réinitialiser l'application pour charger un portefeuille différent.

6. Allez dans le menu "Create" et choisissez "Create New Item". Un menu apparaîtra pour vous demander de télécharger une image gif, jpg ou png. Une fois que vous l'aurez téléchargée sur Freeport, elle ira sur les serveurs d'Imgur et obtiendra sa propre URL.

7. Ensuite, vous devrez nommer votre objet (gardez à l'esprit qu'il s'agit de la description du jeton, et non de son nom), définir la quantité (par exemple, la collection Leftist Tears a une quantité limitée à 21 cartes par édition) et décider si oui ou non vous voulez que l'objet devienne divisible (sera-t-il échangé en unités entières ou permettra-t-il également des fractions ?) Ensuite, vous devez choisir entre un priority fee et un economy fee – il s'agit d'estimations basées sur l'observation par le portefeuille lui-même du mempool des transactions Bitcoin. Pour définir manuellement les frais en fonction de votre propre analyse et de votre préférence temporelle, retournez au menu "Set transaction fees manually".

8. Une fois que vous avez fini de définir les paramètres, appuyez sur le bouton "Create". Si vous avez suffisamment de BTC dans votre portefeuille pour payer les frais de transaction, la transaction OP_RETURN sera diffusée sur le réseau Bitcoin et attendra une confirmation. Après la première confirmation du réseau, votre NFT apparaîtra dans la section "Collect" de Freeport. Vous pouvez l'envoyer aux personnes qui partagent leur adresse Bitcoin avec vous, mais le portefeuille Freeport n'est pas assez avancé pour vous permettre de mettre en place un distributeur pour le vendre. Vous pouvez également recevoir des NFT de vos connaissances en partageant l'une de vos adresses avec eux. Mais si vous voulez exploiter tout le potentiel du protocole Counterparty, vous devrez utiliser un portefeuille avancé comme la version desktop de FreeWallet.io.

Créez Et Gérez Vos NFT Bitcoin Avec La Version Desktop De FreeWallet.Io (Mac, Windows Et Linux)

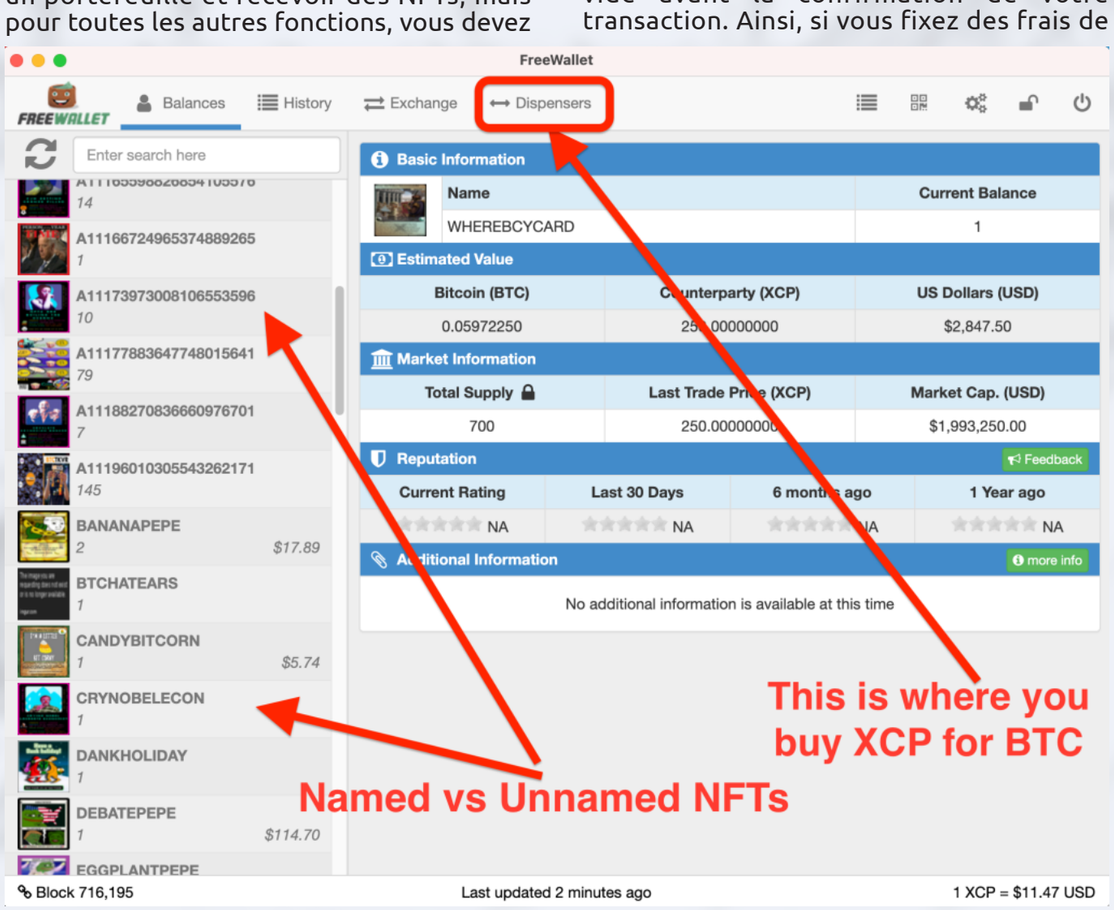
La deuxième méthode, un peu plus compliquée, d'émettre et de gérer des NFTs Bitcoin nécessite un portefeuille desktop comme FreeWallet.io. Si vous voulez que votre nouvel actif porte un certain nom, si vous souhaitez accéder aux dispensers et si vous voulez également verser des dividendes aux détenteurs de vos NFTs, alors vous devez vous tourner vers cette option.

Avant d'entrer dans les détails, vous devez savoir que les versions mobiles du logiciel FreeWallet.io n'ont pas été mises à jour depuis des années et qu'elles présentent certainement des bugs indésirables. Elles conviennent pour générer un portefeuille et recevoir des NFTs, mais pour toutes les autres fonctions, vous devez utiliser votre ordinateur (ou tout appareil fonctionnant sous MacOS, Windows ou Linux).

Pour nommer vos actifs, vous aurez besoin de 0,5 XCP (le jeton utilitaire natif de Counterparty). Et comme les exchanges ne le listent plus, le seul moyen d'acquérir des XCP reste de se tourner vers les dispensers.

Un dispenser c'est un peu comme un distributeur automatique : quelqu'un verrouille une quantité arbitraire d'un actif et permet à tous ceux qui envoient le bon montant de bitcoins d'obtenir la propriété de cet actif. Vous voyez ce que vous voulez acheter, vous choisissez l'offre qui vous satisfait, puis vous procédez à l'achat.

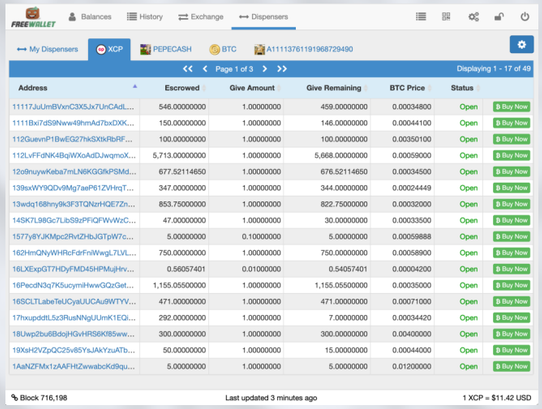
Les dispensers sont des espèces de smart contracts basiques. Mais leur caractère automatisé s'accompagne d'une contrepartie : il y a toujours un risque que le dispenser se vide avant la confirmation de votre transaction. Ainsi, si vous fixez des frais de



transaction trop peu élevés et que vous attendez donc quelques jours avant la première confirmation, vous vous exposez au risque de traiter avec un dispenser fermé ou vidé. La transaction en bitcoin ne peut pas être annulée et il n'y a pas de mécanisme en place pour vous rendre votre argent si la totalité des jetons Counterparty est vendue avant que vous n'ayez pu mettre la main sur l'actif numérique souhaité.

C'est pourquoi vous devriez idéalement payer des frais de transaction plus élevés, afin de vous assurer que vous êtes parmi ceux qui bénéficient d'un bon deal. Vous devriez également essayer de n'acheter qu'auprès des dispensers créés par des adresses que vous reconnaissez. Si vous connaissez le propriétaire et que vous vous fiez à sa réputation, vous avez plus de chances de récupérer vos bitcoins si l'échange n'a pas lieu.

J'ai perdu environ 40 $ de bitcoins en essayant d'acheter des XCP pour nommer mes NFTs : la première fois, le dispenser a été fermé avant que je puisse recevoir ma première confirmation (arnaque classique) ; la deuxième fois, quelqu'un a acheté tous les XCP du distributeur avant que ma première confirmation n'arrive. Dans les deux cas, je n'avais aucune idée d'avec qui j'étais en train de traiter et je ne savais pas comment contacter le propriétaire. C'est malheureux, mais ça fait partie de tout marché numérique décentralisé, non réglementé et libre.

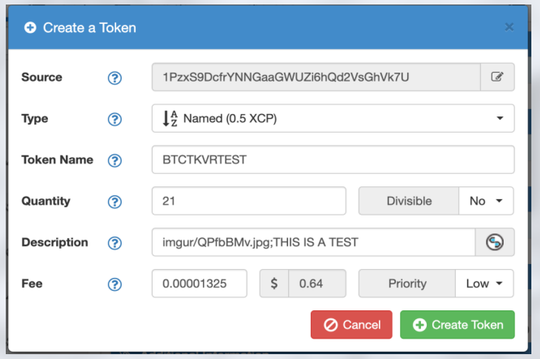


Après avoir acquis votre premier XCP (n'oubliez pas que vous avez besoin de 0,5 par NFT auquel vous allez attribuer un nom et que vous devez l'utiliser dès que possible plutôt que de l'utiliser à des fins spéculatives), allez dans le menu "Actions" en haut à droite de la fenêtre de FreeWallet et choisissez "Create a Token".

Ici, vous allez devoir sélectionner l'adresse source et le type d'actif (named, subasset, ou numeric). Vous devez également saisir le nom de votre jeton et sa quantité (qui peut au choix être divisible ou non).

Ensuite, vous devez préciser une description. Et c'est ici que vous indiquez votre fichier image à FreeWallet. Vous allez devoir apprendre à utiliser la bonne syntaxe, car la structure est "imgur/imagename.jpg; DESCRIPTION DE VOTRE TOKEN " . Remarquez que vous ne saisissez pas l'URL complète de votre source Imgur ou YouTube, mais que vous utilisez une forme abrégée. En outre, il n'y a pas d'espace avant ou après le point-virgule. C'est très important, car j'ai déjà fait cette erreur et l'image ne s'affichait pas correctement; j'ai dû renvoyer une autre transaction qui a modifié la description.

Il y a une remarque importante à faire ici concernant Imgur et d'autres services centralisés, parce qu'ils sont en mesure de censurer et supprimer votre image. Cependant, vous pouvez la télécharger ailleurs et modifier la description de votre jeton par une transaction en BTC. C'est pourquoi on dit que le jeton est l'oeuvre – parce que si l'actif Counterparty est immuable et ne peut pas être renommé, la description peut être modifiée à tout moment pour le prix d'une transaction on-chain.



Enfin, vous devez fixer des frais de transaction qui correspondent à votre préférence temporelle. Idéalement, vous

devriez vous assurer qu'elle est confirmée dans les deux semaines afin que la plupart des nœuds ne la suppriment pas de leur mempool. Mais les frais de priorité faible ou moyenne recommandés par mempool.space devraient suffire pour minter votre NFT en quelques heures.

Notez que vous ne fixez pas vos frais en utilisant le système classique sat/byte ou bit/kb. Au lieu de ça, vous choisissez le montant total que vous voulez payer comme frais. Gardez à l'esprit que ces transactions OP_RETURN sont généralement plus importantes que le transfert d'argent moyen (elles occupent plus d'espace de bloc) et jetez un coup d'oeil aux recommandations de coût en dollars pour une approximation plus précise. Par défaut, FreeWallet ne vous laissera pas payer des frais inférieurs à 0,00001 BTC (10 bits, ou 1000 sats) par transaction, mais vous pouvez le modifier dans le menu des paramètres.

Une fois que vous avez défini tous ces paramètres, cliquez sur le bouton "Create Token" et c'est parti. Votre NFT sera disponible après que la transaction OP_RETURN correspondante ait reçu sa première confirmation sur la blockchain Bitcoin.



Qu'est-ce que vous pouvez faire ensuite? Vous pouvez l'envoyer à vos connaissances, vous pouvez mettre en place un dispenser pour le vendre, et vous pouvez même en "brûler" une partie pour le rendre encore plus rare. Si vous voulez récompenser les détenteurs de vos jetons, vous pouvez également leur verser des dividendes.

Quant au jeton lui-même, vous pouvez modifier sa description et sa représentation visuelle quand bon vous semble. Mais le nom restera à tout jamais. Tout comme dans le cas des noms de domaine, un élément déjà pris ne pourra pas être utilisé par quelqu'un d'autre – sauf qu'aucun renouvellement périodique n'est nécessaire. Une fois que vous l'avez émis, le nom de l'actif vous appartient. Et en réalité, c'est ce que les gens achètent.

Vous pouvez également côter le jeton sur les exchanges pour XCP – cette fonctionnalité est disponible sur des portefeuilles tels que Counterwallet (eds.counterwallet.io). La liquidité pour les nouveaux NFTs est vraiment faible et c'est probablement préférable d'ouvrir des dispensers qui vous permettent de vendre vos jetons contre du BTC. Mais si vous voulez explorer ce terrier du lapin de la financiarisation et faire plus avec votre XCP, libre à vous d'essayer.

Obtenez Vos Premiers Tokens Sur Counterparty

Dans les jeux Pokemon, quand vous entamez le jeu vous avez le choix entre Salamèche, Bulbizarre ou Carapuce. Il faut bien commencer quelque part, quoi. Là je vous propose de démarrer non pas avec un NFT au sens propre mais avec Moulacoin, un meme coin créé exactement de la même manière qu'expliqué précédemment, qui n'a d'autres prétention que d'encourager les gens à utiliser les assets sur Counterparty et ironiquement ridiculiser les projets "crypto" qui se prennent trop au sérieux.

J'ai mis en place un dispenser qui distribue des milliers de coins si le coeur vous en dit, pour aider à comprendre comment ça fonctionne. C'est simple, il suffit de créer une adresse Counterparty, d'envoyer quelque Sats depuis cette adresse et les

l'auteur de ce ligne et l'encourager à minter d'autres assets.



Mais alors que j'expérimentais avec les dispensers, j'ai découvert que certains portefeuilles Counterparty utilisent l'ancienne dust limit de BTC de 5460 sats. Certes depuis un certain temps déjà, les développeurs de Bitcoin Core l'ont fixée à 546 sats, mais certains portefeuilles Counterparty pas mis à jour peuvent parfois encore conserver l'ancienne limite.

Ça signifie que toute transaction inférieure à 0,00005460 BTC peut ne pas être diffusée sur le réseau. Si ça se produit, et que vous envisagez d'acheter un asset inférieur à ce prix alors vous devrez en acquérir plusieurs à la fois.

Quoi qu'il en soit, l'objectif de ce meme coin est d'aider autant de personnes que possible à obtenir leur premier asset sur Counterparty au dessus de Bitcoin et comprendre comment tout ça fonctionne. Je n'encourage clairement pas la spéculation avec. Pour faciliter le tout j'ai crée un QR code qui mène au dispenser et pour avoir des info sur cet actif (ou n'importe lequel autre d'ailleurs), il suffit de se rendre sur xchain.io et de taper MOULACOIN (un onglet "dispenser" vous y attend si nécessaire)

Les NFT de Counterparty sont une façon amusante de jouer avec Bitcoin. Vous pouvez explorer les caractéristiques d'un des premiers protocoles qui visait à intégrer tout un éventail d'actifs financiers à Bitcoin. Vous pouvez également découvrir par où tout cet engouement a commencé, rejoindre les groupes Telegram et devenir amis avec les OG qui ont créé Rare Pepes et Spells of Genesis (que vous pouvez également entendre dans la saison 10 du podcast Bitcoin Takeover).

Mais pour ce qui me concerne, c'est important de prouver que Bitcoin est bien plus qu'un outil financier. C'est aussi un réseau informatique distribué qui permet la

coins seront transférés sur votre wallet (10,000 coins pour 0.0001 BTC pour être exact)

Pourquoi je ne les distribue pas gratuitement ? Eh bien, je l'ai fait par le passé via twitter mais techniquement c'est compliqué ici de le faire pour des gens dont j'ignore l'existence – à moins que vous ne m'envoyiez votre adresse Bitcoin Counterparty par message privé, que je fasse une liste, puis que j'envoie des transactions par lots aux destinataires intéressés. En plus, le but ici est de vous enseigner le fonctionnement des NFTs et autres actifs de manière rapide et abordable. Et tous les fonds reçus seront quoi qu'il arrive utilisés pour créer d'autres NFTs ou mockcoins qui seront eux distribués gratuitement.

Ainsi, après avoir crédité votre FreeWallet d'au moins 0,0001 BTC (le montant minimum pour acheter les coins) et d'environ 0,00001000 BTC pour les frais de transaction, vous pouvez utiliser le dispenser pour "échanger" vos coins. Bien sûr, vous pouvez en acquérir plus si vous souhaitez soutenir



liberté d'expression. Des messages qui seraient autrement censurés ou supprimés peuvent faire leur chemin sur le réseau Bitcoin – moyennant des frais de transaction, bien entendu. Mais les intentions ne sont pas toujours financières et il existe de nombreuses façons de s'exprimer via Bitcoin (les NFT de Counterparty étant simplement l'une d'entre elles).



Comme l'a mentionné Justin Wales, avocat américain spécialiste du premier amendement, dans le S5E4 du podcast Bitcoin Takeover, Bitcoin c'est la liberté d'expression et devrait être protégé à travers les dispositions de la Constitution américaine et de la Bill of Right. Donc, si nous rendons les utilisations non financières du réseau Bitcoin plus courantes, alors nous renforçons cette thèse et gagnons des batailles importantes contre les régulateurs qui semblent ne prêter l'oreille qu'à des récits trop simplifiés. Bitcoin n'est pas une marchandise, ce n'est pas une security, il ne ressemble à rien de ce que les systèmes juridiques ont jamais vu jusqu'à maintenant et il peut être utilisé pour exercer sa liberté d'expression ou même s'amuser.

Quel Est L'intérêt Des NFT ?

Bien sûr, ces cas d'utilisation ne conviennent pas à tout le monde. Si vous êtes adepte de la thésaurisation et du HODLing de BTC, vous ne comprendrez pas les NFT.

Et c'est très bien ainsi, tout le monde n'aspire pas à collectionner des cartes

virtuelles et ne trouve pas de valeur dans des jetons arbitraires sur le réseau Bitcoin avec éventuellement un jpeg ou un gif attaché.

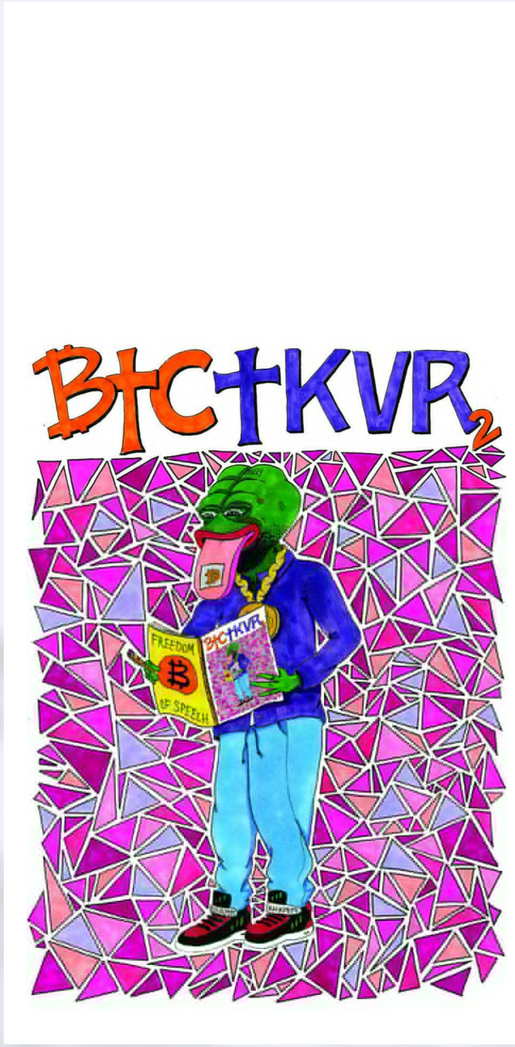
Les NFTs ne sont pas une classe d'actifs, ce ne sont pas des "pièces de monnaie", et ils ne ressemblent pas non plus tout à fait aux cartes de baseball à collectionner.

Ce sont des objets de collection rares qui racontent une histoire, qui ont un sens pour le collectionneur ou qui permettent simplement aux bitcoiners les plus riches de soutenir le travail d'un jeune artiste.



Et même s'il existe un marché spéculatif sur les NFTs, leur but n'est pas toujours financier – il s'agit parfois simplement de s'amuser en tant que nerd de manière coûteuse.

Tous les NFTs ne sont pas égaux et c'est là tout l'intérêt d'un objet "non fongible". Il est unique à sa manière, présente des particularités que d'autres peuvent trouver attrayantes au point de payer de l'argent, et évoque un certain sentiment ou souvenir.



Certains sont historiques, d'autres sont amusants, mais tous rappellent que la communauté Bitcoin est vraiment fun et diverse.

La prochaine fois que quelqu'un vous parlera d'une collection sympa sur Ethereum ou Solana, rappelez-lui que Bitcoin l'a fait en premier et le fait encore mieux avec Counterparty.

Et si jamais l'envie vous prend de m'envoyer certaines de vos créations, mon adresse est bc1ql9vxydvsvclva4mzhw3yu89ddekqqwj9ydmqg4.



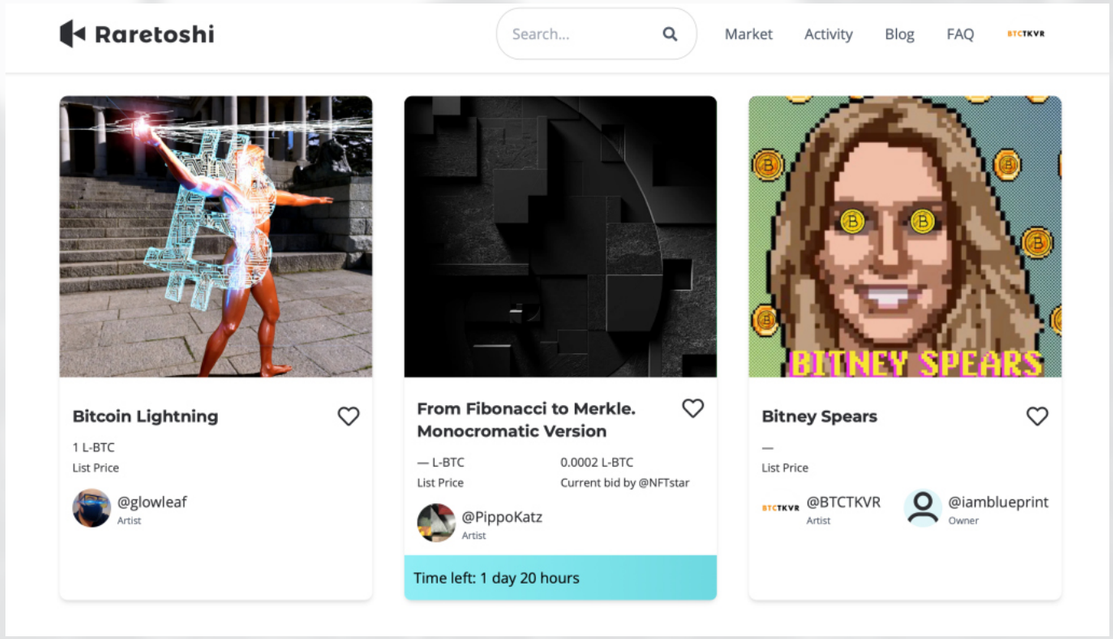
Raretoshi: Des NFTs Bitcoin Sur La Sidechain Liquid

Raretoshi est une marketplace de NFT qui utilise la sidechain Liquid de Blockstream pour fournir des transactions confidentielles, peu coûteuses et extensibles. Cette plateforme est un peu l'héritière spirituelle de Counterparty (le protocole Bitcoin qui a été le pionnier de l'ouragan des NFTs avec ses cartes de collection et ses memes) et a pour ambition de permettre des enchères transparentes pour les oeuvres d'art numériques limitées.

Nous sommes en 2022, et toutes les blockchains jamais créée tentent aujourd'hui de capitaliser sur la frénésie NFT. Et pendant qu'Ethereum est confronté à des problèmes de scalabilité et de frais excessifs tout en maintenant une politique monétaire discutable (la démonstration la plus récente de son imprévisibilité étant l'EIP1559), d'autres réseaux utilisent leurs capacités afin de permettre l'émergence de marketplaces NFT pratiques et abordables.

Il y a deux raisons essentielles pour lesquelles Raretoshi est meilleur qu'Opensea, Rarible et toutes les autres plateformes concurrentes: tout d'abord, elle utilise la cryptomonnaie la plus dure, la plus décentralisée, et la plus liquide du monde. Et tandis que certains pourraient soutenir que des jetons à parité fixe avec bitcoins ne sont pas des vrais bitcoins car ils ne transitent pas sur sur le réseau Bitcoin, il est important de noter qu'il existe un ancrage démontrable de 1 pour 1 entre les BTC et les L-BTC. Par conséquent chaque montant utilisé pour les transactions existe d'autre part dans un contrat verrouillé Bitcoin.

Deuxièmement, Raretoshi rend possible les dépôts via Confidential Transaction (un protocole qui aboutit au cryptage du montant). Cela implique que vous pouvez faire des versements sur votre compte sans toutefois révéler au reste du monde combien de bitcoins vous avez affecté à la plateforme. J'estime personnellement qu'Ethereum est



un cauchemar Orwellien en raison de son modèle "une adresse par wallet" qui rend l'ensemble des transactions aisément traçables. Et comme le monde de l'art intègre des ventes aux enchères où les enchérisseurs souhaitent conserver l'anonymat, Liquid est mieux adapté à la gestion de ce type de transactions.

Toutefois, certaines critiques relatives à l'anonymat fourni lors des transactions sur Liquid doivent être abordées: en raison de la situation actuelle avec ses blocs quasiment vides, il est facile d'affiner la liste des suspects. Un analyste des réseaux sociaux peut surveiller Twitter afin de déceler quels utilisateurs notoires de Liquid sont adeptes de la confidentialité, tandis qu'un analyste blockchain peut vérifier combien de bitcoins ont été permutés pour un usage sur la sidechain et de quels UTXO ils proviennent. Et puisque la confidentialité n'est pas paramétrée par défaut, la plupart des transactions ne l'utilisent pas (soit par ignorance, ou soit pour réduire les coûts ou bien l'espace utilisé par bloc).

Pourquoi Raretoshi Est Positif Pour Liquid La Sidechain De Bitcoin

Quelle que soit votre opinion sur les NFTs et l'approche que vous choisissez vis à vis de la bulle existante sur l'art numérique tokénisé, il est indéniable que ces actifs cryptographiques augmentent l'activité économique. C'est une excellente nouvelle pour Liquid, puisqu'un nombre croissant d'utilisateurs verrouilleront leur bitcoins pour obtenir des L-BTC, effectueront des transactions, et s'acquitteront de frais envers les producteurs fédérés de blocs.

Il s'agit potentiellement d'une coincidence, mais entre Juillet et Août 2021, la quantité de bitcoins permutés sur la sidechain Liquid a augmenté, passant de 2940 à 3213. Bien qu'il soit possible que les 273 L-BTC supplémentaires soient dûs à la poursuite du marché haussier (les membres de la fédération Liquid ont peut-être décidé de s'éviter de payer des frais de transaction élevés dans les périodes où le demande pour le block space culmine), on ne peut aussi pas écarter la probabilité que cela soit dû à la popularisation du phénomène NFT.

Assurément, Liquid a besoin de plus d'utilisateurs et de plus de transactions de la part d'usagers réguliers. Les exchanges n'ont pas besoin de faire du settlement très fréquemment, et pour cette raison beaucoup de blocs demeurent vides entre les transferts. Ainsi, pourquoi ne pas utiliser ce

block space supplémentaire pour émettre des NFTs et faire des transactions qui leur seraient associées? On ne peut pas dire que le poids que représenterait le stockage d'une masse supérieure de données affecterait tellement les membre de la fédération qu'il leur en deviendrait alors impossible de faire tourner un noeud – après tout, ce sont des exchanges et des sociétés qui peuvent s'offrir d'améliorer leurs capacités de stockage.

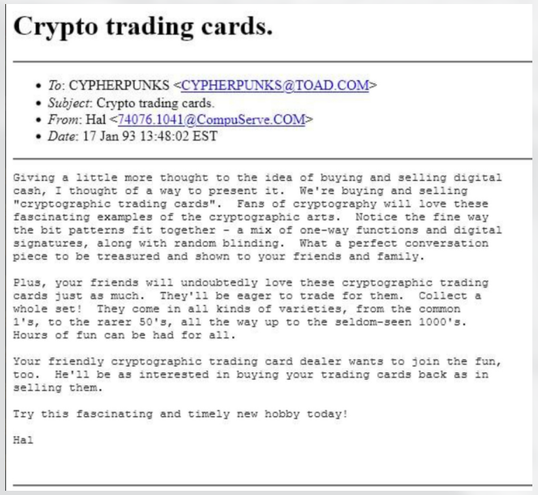
Mais si Liquid réussit en tant que sidechain fédérée, alors elle va probablement mettre en lumière d'autres projets et pousser leur développement. RSK (appelé précédemment Rootstok) est un exemple parfait de projet qui tente d'amener les smart contracts d'Ethereum sur Bitcoin, mais ne bénéficie pas vraiment encore d'effet de réseau et aurait besoin de davantage de publicité. De même, la proposition de Drivechain de Paul Sztorc (BIP 300 & 301) ou de Statechain de Ruben Somsen pourraient également profiter du succès de Liquid, en voyant leur développement s'accélérer pour répondre à la demande.

Finalement, Raretoshi est une tentative de ramener les futures Bitcoin sur Bitcoin – mais d'une manière flexible, privée et économique qui peut répondre aux demandes du marché d'une façon plus élégante. Si cela venait a être un succès, alors cela rendrait également plus populaire les sidechains pour les activités économiques des utilisateurs individuels. Et si Liquid devenait populaire, alors il est probable aussi que les Confidential Transactions (ou une de leur approche plus évolutive) recevraient plus de soutien et de demande de la part des utilisateurs concernant la couche de base de Bitcoin. Sans vouloir rajouter de pression, il se pourrait que cette marketplace de NFT puisse changer la donne.

C'est Quoi Cet Engouement Autour Des NFTs?

Cet article a été publié pour la premiére fois en Août 2021 et nous nous trouvions en plein milieu d'une bulle de l'art numérique et des NFTs qui ressemblait précisément à la frénésie des ICOs de 2017-2018. Il est fort probable que les travaux exposés étaient largement surévalués et recevaient un tel niveau d'attention uniquement pour des raisons spéculatives. En effet, fondamentalement les NFTs ne sont rien de plus que des hashes cryptographiques qui sont minés dans des transactions on-chain et qui sont supposés avoir un objet numérique ou physique associé.

Par exemple, des NFTs du magazine BTCTKVR en Anglais ont été mis en vente accompagné de sa livraison en version papier. Les plus offrant pour le numéro 1 sur 21 ont pu de fait revendiquer la propriété sur le réseau Liquid de l'asset numéro 9f35eec7884174b2f338763d827192966b6a680704c0553f865e30e2994a60e0 , inclus dans le bloc 1447855, le 17 Août 2021. Ca n'a pas l'air très excitant parce qu'en vérité ça ne l'est pas vraiment – mais il y a quelque chose de magique avec les nombres et certains collectionneurs apprécient la valeur que représente l'exclusivité vérifiable de ce hash cryptographique. C'est comme des cartes à collectionner mais pour les geeks. De plus, dans ce cas précis, la livraison d'un magazine dans son format physique était inclus de façon à ce que l'enchérisseur ne se sente pas arnaqué ou trompé par un phénomène surestimé.



Crypto trading cards.

- *To*: CYPHERPUNKS <CYPHERPUNKS@TOAD.COM>
- *Subject*: Crypto trading cards.
- *From*: Hal <74076.1041@CompuServe.COM>
- *Date*: 17 Jan 93 13:48:02 EST

Giving a little more thought to the idea of buying and selling digital cash, I thought of a way to present it. We're buying and selling "cryptographic trading cards". Fans of cryptography will love these fascinating examples of the cryptographic arts. Notice the fine way the bit patterns fit together - a mix of one-way functions and digital signatures, along with random blinding. What a perfect conversation piece to be treasured and shown to your friends and family.

Plus, your friends will undoubtedly love these cryptographic trading cards just as much. They'll be eager to trade for them. Collect a whole set! They come in all kinds of varieties, from the common 1's, to the rarer 50's, all the way up to the seldom-seen 1000's. Hours of fun can be had for all.

Your friendly cryptographic trading card dealer wants to join the fun, too. He'll be as interested in buying your trading cards back as in selling them.

Try this fascinating and timely new hobby today!

Hal

Et pourtant l'élément intéressant des NFTs réside dans le fait que que l'artiste recevra un pourcentage défini de manière arbitraire sur l'ensemble des transactions ultérieures. Ainsi, si un artiste vend son travail pour une somme de 0.01 L-BTC et fixe un montant de royalties de 10%, et que par la suite le collectionneur revend son travail pour 1 L-BTC, l'artiste recevra de son côté 0.1 L-BTC sur cette nouvelle transaction. C'est un modèle plutôt habile qui résout en partie le problème de l'artiste fauché – si l'on produit une oeuvre véritablement précieuse et intemporelle, il devient alors possible de vivre de cette création au gré de ses transactions.

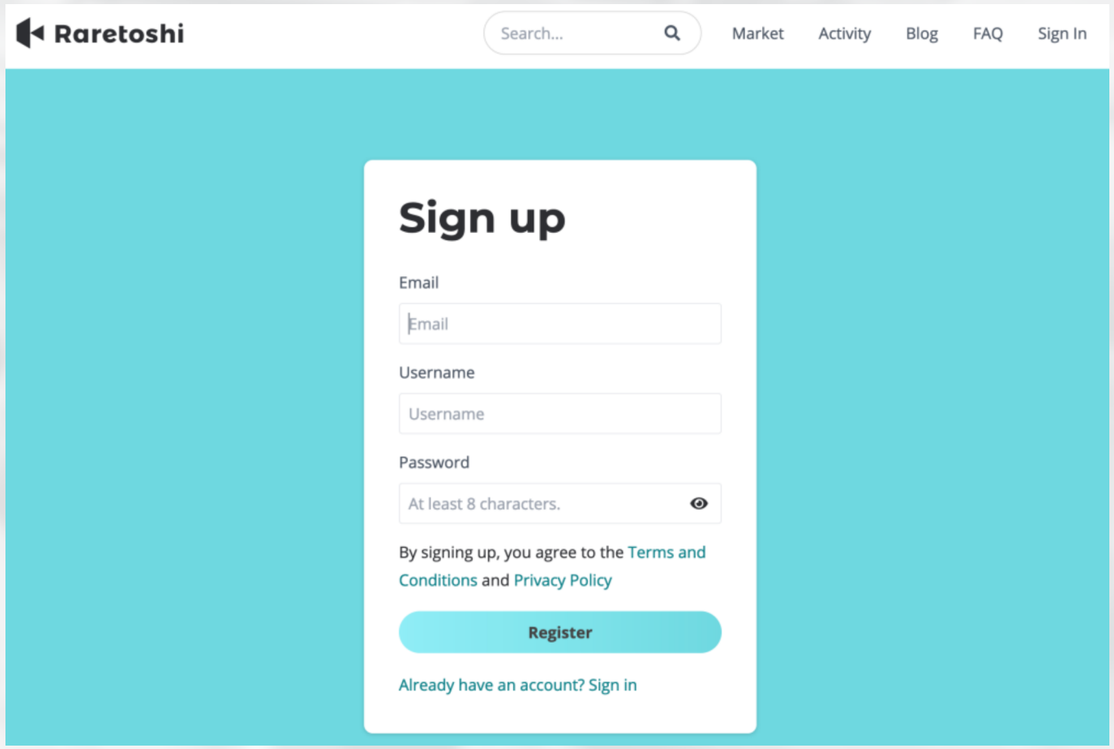
Naturellement, cet environnement attire des spéculateurs uniquement à la recherche d'oeuvres d'art numérique dans l'optique de les revendre ultérieurement en réalisant un profit. Et bien qu'absolument rien ne soit répréhensible dans la dynamique de libre marché, savoir que les artistes vendent principalement leurs oeuvres avec l'espoir de bénéfices périodiques et que des influenceurs tirent avantage de leur position pour prendre part au même exercice de pump and dump que l'on a pu voir dans les autres cycles de bull market, peut apparaitre comme inconsistant.

En outre, de nombreuses oeuvres donnent le sentiment d'être bâclées et leur mise sur le marché précipitée – des indicateurs qui rappellent la vision de court terme que Bitcoin entend rectifier. Mais il y a fort à parier que l'on va tendre vers un marché moins exubérant et plus rationnel, une fois que cette bulle NFT aura éclaté et que tout le monde aura reçu un douloureux rappel concernant les fondamentaux et les raisons pour lesquels nous élaborons ces technologies.

Comment Configurer Votre Compte Sur Raretoshi

Pour vous inscrire sur Raretoshi, vous devez fournir une adresse email, un identifiant et un mot de passe. Ce mécanisme d'identification old school n'est certes pas idéal et cela serait clairement bien plus intéressant si les utilisateurs pouvaient utiliser leur noeud Lightning pour prouver leur identité. Mais cette architecture est la plus courante et à l'avantage de ne pas représenter un frein pour les nouveaux utilisateurs.

Après avoir saisis vos identifiants et cliqué sur "Register", vous allez devoir confirmer votre inscription depuis votre adresse email. Une fois cette confirmation



effectué, un seul clic suffit pour naviguer entre les différents NFTs Bitcoin et apporter votre support à quelques uns des meilleurs projets artistiques numériques (et même parfois physiques) de l'écosystème.

Passé ce processus d'enregistrement, on peut distinguer deux sections sur le site: la marketplace NFT dans laquelle on peut naviguer avec un menu relativement simple qui n'est pas tellement différent de celui d'eBay ou d'autres site d'enchères, et le wallet L-BTC. Bien que le site soit centralisé, votre wallet Liquid est non-custodial et génère en fait une seed de 12 mots (BIP 39) afin de vous laisser la responsabilité de la gestion de vos fonds.

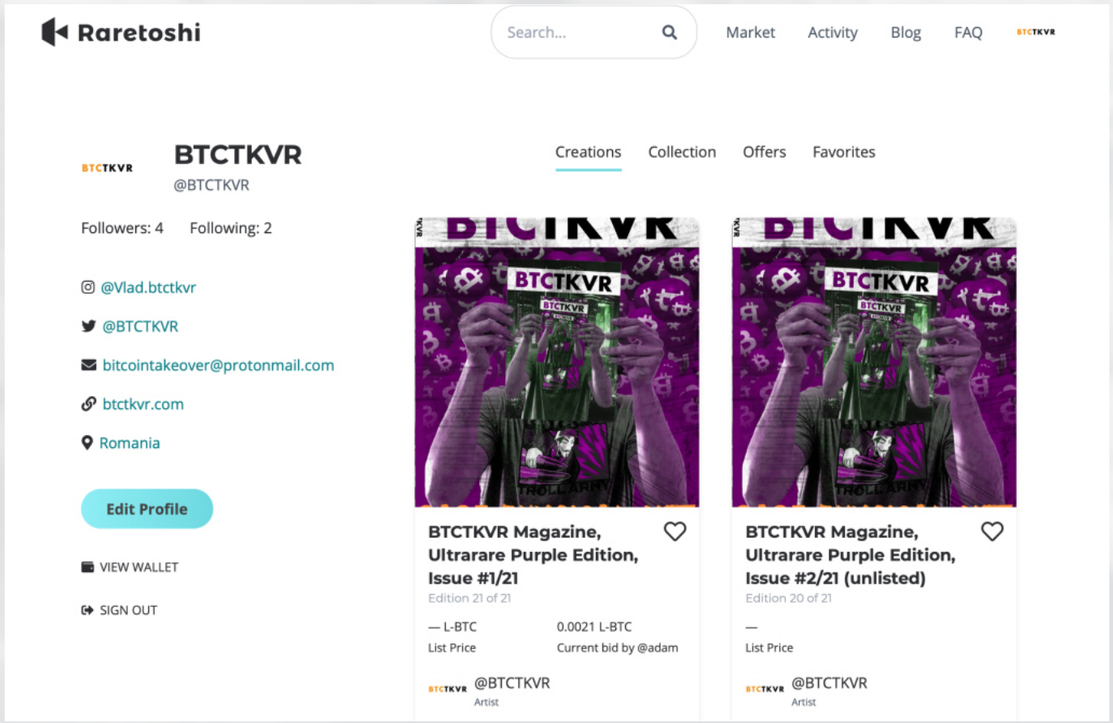
Par conséquent on peut aisément considérer Raretoshi comme rien de plus qu'une interface qui facilite l'achat d'art numérique sous forme de NFT. On peut ajouter qu'il ne s'agit pas non plus d'un service qui conserve en custody vos bitcoins permutés sur la sidechain. Ainsi, si jamais vous souhaitez récupérer vos fonds et les dépenser dans un autre wallet Liquid tel que AQUA de Blockstream, vous avez la possibilité de le faire sans aucuns soucis.

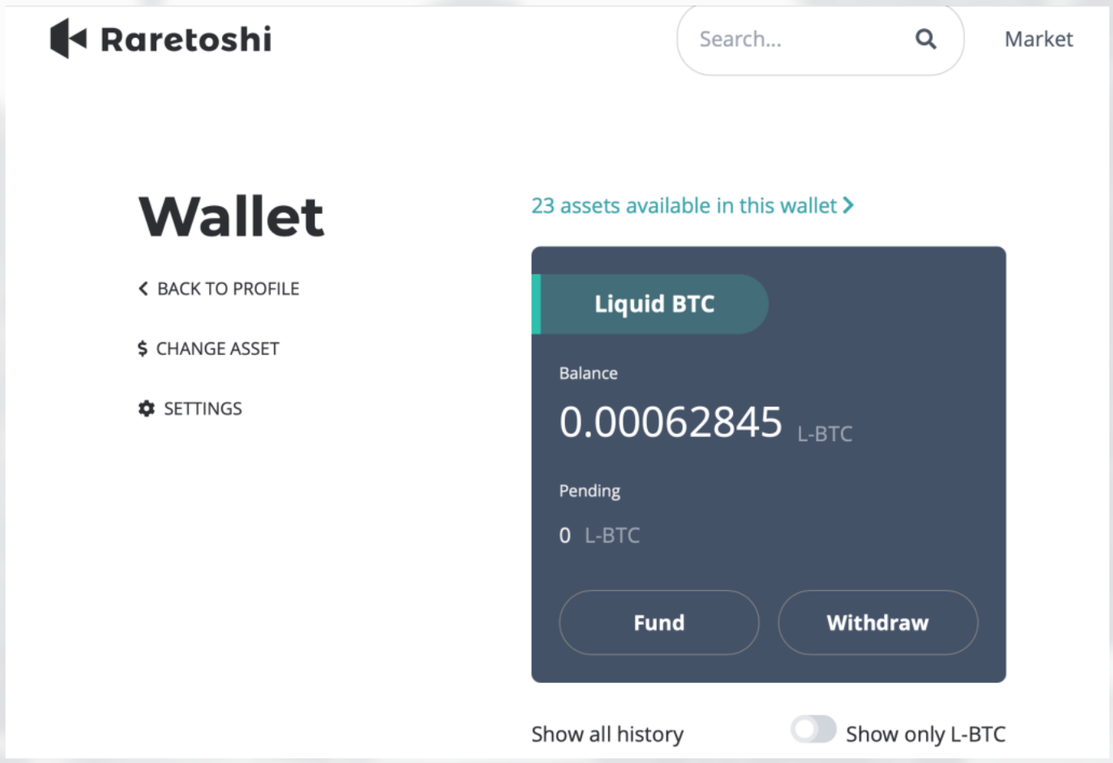
Le menu supérieur contient un champs de de recherche, une section marketplace où sont exposés les oeuvres selon des critères de nouveauté, de prix ou de popularité, ainsi qu'un onglet affichant les dernières activités (dernières enchères et dernières ventes achevées). Pour ceux désirant en savoir davantage, il existe un blog qui met en avant quelques unes des oeuvres les plus intéressantes, ainsi qu'une section FAQ fournissant des explications pratiques.

Dans un premier temps, il est uniquement possible d'acheter des NFTs sur la marketplace. Les artistes devront eux se plier à un processus de vérification spécifique au cours duquel ils devront soumettre certaines de leurs oeuvres.

Dans mon cas, cette procédure de vérification a été relativement rapide et j'ai eu affaire à des administrateurs aimables et attentionnés.

Il sera toutefois intéressant d'observer comment cela va évoluer lorsque la plateforme deviendra plus populaire et que les demandes de publication d'œuvres commenceront à affluer.





Depuis l'interface de leur compte, les utilisateurs peuvent consulter leurs collections, parcourir les offres et également garder un œil sur leurs œuvres d'art préférées. Il s'agit d'un design simple et minimaliste qui ne nécessite aucune explication ni aucune courbe d'apprentissage.

Penchons nous maintenant sur la partie wallet. Grâce à Raretoshi, les NFTs peuvent être émis et échangés en utilisant la monnaie la plus dure de cette planète.

Et grâce à l'aide d'intermédiaires qui vous permettent de permuter rapidement vos BTC contre des L-BTC (et vice-versa) en échange d'une commission minime, l'intégration sur la plateforme ne nécessite pas de faire tourner un nœud L-BTC et d'attendre 100 confirmations du réseau pour compléter cette permutation.

Raretoshi vous permet de déposer des BTC soit via la base layer, soit via le réseau Lightning – il existe certes un léger risque de contrepartie lorsque vous utilisez Coinos (l'intermédiaire sélectionné par défaut), mais si vous préférez vous pouvez opter pour l'utilisation d'autres services tels que Liquiditi, SideShift AI, Bisq, Flip.me et SideSwap. Autrement, vous avez également la possibilité d'acheter des L-BTC avec votre carte de crédit directement à partir du wallet AQUA de Blockstream sur mobile.

Gardez bien à l'esprit que vous devez protéger votre seed phrase BIP39, car le wallet généré par Raretoshi peut être accessible via l'ensemble des logiciels compatibles avec le réseau Liquid (y compris AQUA de Blockstream).

Pour relater ma propre expérience, je n'ai pas été en mesure de récupérer mon wallet dans Green de Blockstream car ce wallet utilise une configuration multisignature de 2 sur 2, fonction qui n'est pas supporté par Raretoshi (en tout cas pas encore).

Si vous engrangez beaucoup de L-BTC en vendant des NFTs et que vous souhaitez les stocker en tant que tels, il est fortement recommandé de vous procurer le hardware wallet Jade de Blockstream afin mieux les sécuriser.



Le Vol De 3094 Bitcoins Qui A Conduit À La Création Du Trezor

Remontons en 2012; il s'agissait d'une époque beaucoup plus insouciante pour les HODLers de bitcoins. En fait, pour être vraiment précis on ne peut pas vraiment les appeler ainsi puisqu'il faudra encore attendre un an et demi avant que le terme "HODL" ne soit inventé par GameKyuubi, un amateur de whisky adepte du forum de bitcointalk.

On parle des débuts, quand le prix d'un BTC oscillait entre 4 et 13 dollars sur une année entière.

L'amplitude de volatilité qu'on observe aujourd'hui sur quelques secondes correspond à la totalité de la capitalisation du bitcoin de cette époque – et la plupart des utilisateurs n'étaient encore que des cypherpunks, des nerds et des libertariens.

Par conséquent, les gens étaient beaucoup plus détendus en matière de sécurité et n'envisageaient pas tous les vecteurs de menace qui nous rendent aujourd'hui tous si méfiants.

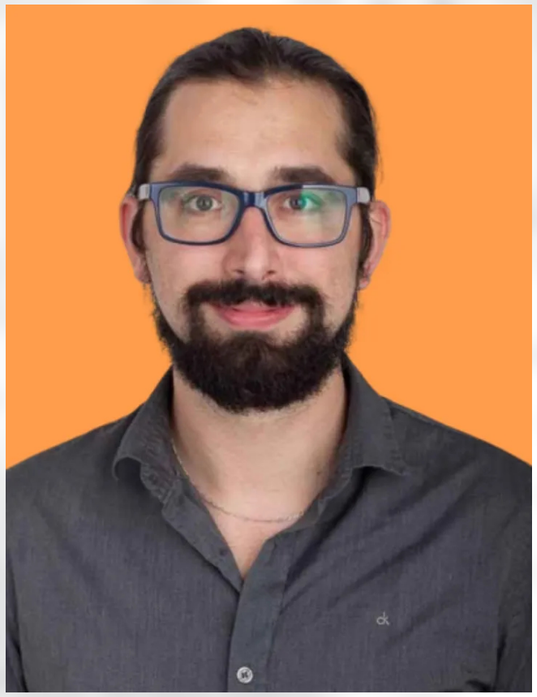
La perte de coins était beaucoup plus courante, car même les utilisateurs les plus techniques étaient négligents dans leur utilisation de wallets.

À leur décharge, il faut dire qu'à ce moment là les wallets exigeaient des utilisateurs qu'ils récupèrent les fichiers wallet.dat (qt pour Bitcoin), qu'ils scannent les codes QR des clés privées (pour les portefeuilles mobiles) ou qu'ils saisissent les clés manuellement (difficile à imaginer mais des personnes effectuaient des paiement en saisissant eux même les adresses).

Il faudra attendre encore un an et demi avant que ne soit inventé le standard BIP39, qui permet aujourd'hui aux utilisateurs de convertir leurs clés privées en mots mnémoniques tirés d'un dictionnaire.

1er Mars 2012 – Les Serveurs Backup Linode De Slush Pool Sont Hackés, 3094 BTC Disparaissent

Au début de l'année 2012, Marek "Slush" Palatinus dirigeait les opérations de Slush

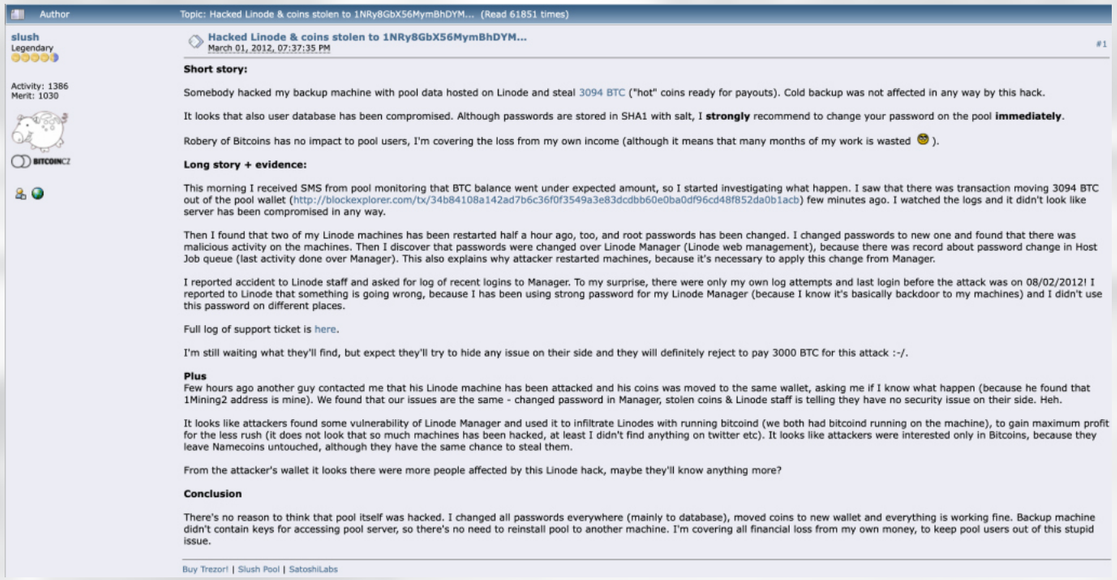


Pool (la première pool de minage au monde, comme l'a reconnu Satoshi lui-même) avec un peu d'aide de Linode la société d'hébergement Cloud. Tout semblait aller pour le mieux jusqu'au 1er mars 2012, quand Slush a reçu un message inattendu du service de surveillance de sa pool – apparemment, sa réserve de bitcoins avait été vidée de manière inattendue.

Après investigation, le cypherpunk tchèque découvrit que deux des serveurs Linode qu'il utilisait pour sauvegarder les données de la pool de minage étaient corrompus – quelqu'un les avait redémarrés et avait changé leurs mots de passe administrateur.

Le problème était dû à une vulnérabilité du logiciel de gestion de Linode – cela n'avait rien à voir avec la sécurité du logiciel Bitcoin ou du protocole de la pool de minage. Il est probable que Bitcoin était en train de devenir un sujet en vogue chez les hackers, car plusieurs autres instances de Linode exécutant bitcoind avaient été ciblées à peu près au même moment.

Au total, 50 000 BTC ont été volés des serveurs Linode le 1er mars 2012 – marquant ainsi le plus grand vol de bitcoins jusqu'à nos jours. Et tout cela est arrivé à cause d'une mise à jour de sécurité qui a été exploitée avec succès par les hackers. Même le faucet bitcoin de Gavin Andresen, qui distribuait



Author | Topic: Hacked Linode & coins stolen to 1NRy8GbX56MymBhDYM... (Read 61851 times)

slush
Legendary
Activity: 1386
Merit: 1030

Hacked Linode & coins stolen to 1NRy8GbX56MymBhDYM...
March 01, 2012, 07:37:35 PM #1

Short story:

Somebody hacked my backup machine with pool data hosted on Linode and steal 3094 BTC ("hot" coins ready for payouts). Cold backup was not affected in any way by this hack.

It looks that also user database has been compromised. Although passwords are stored in SHA1 with salt, I **strongly** recommend to change your password on the pool **immediately**.

Robery of Bitcoins has no impact to pool users, I'm covering the loss from my own income (although it means that many months of my work is wasted).

Long story + evidence:

This morning I received SMS from pool monitoring that BTC balance went under expected amount, so I started investigating what happen. I saw that there was transaction moving 3094 BTC out of the pool wallet (http://blockexplorer.com/tx/34b84108a142ad7b6c36f0f3549a3e83dcdbb60e0ba0df96cd48f852da0b1acb) few minutes ago. I watched the logs and it didn't look like server has been compromised in any way.

Then I found that two of my Linode machines has been restarted half a hour ago, too, and root passwords has been changed. I changed passwords to new one and found that there was malicious activity on the machines. Then I discover that passwords were changed over Linode Manager (Linode web management), because there was record about password change in Host Job queue (last activity done over Manager). This also explains why attacker restarted machines, because it's necessary to apply this change from Manager.

I reported accident to Linode staff and asked for log of recent logins to Manager. To my surprise, there were only my own log attempts and last login before the attack was on 08/02/2012! I reported to Linode that something is going wrong, because I has been using strong password for my Linode Manager (because I know it's basically backdoor to my machines) and I didn't use this password on different places.

Full log of support ticket is here.

I'm still waiting what they'll find, but expect they'll try to hide any issue on their side and they will definitely reject to pay 3000 BTC for this attack :-/.

Plus
Few hours ago another guy contacted me that his Linode machine has been attacked and his coins was moved to the same wallet, asking me if I know what happen (because he found that 1Mining2 address is mine). We found that our issues are the same - changed password in Manager, stolen coins & Linode staff is telling they have no security issue on their side. Heh.

It looks like attackers found some vulnerability of Linode Manager and used it to infiltrate Linodes with running bitcoind (we both had bitcoind running on the machine), to gain maximum profit for the less rush (it does not look that so much machines has been hacked, at least I didn't find anything on twitter etc). It looks like attackers were interested only in Bitcoins, because they leave Namecoins untouched, although they have the same chance to steal them.

From the attacker's wallet it looks there were more people affected by this Linode hack, maybe they'll know anything more?

Conclusion

There's no reason to think that pool itself was hacked. I changed all passwords everywhere (mainly to database), moved coins to new wallet and everything is working fine. Backup machine didn't contain keys for accessing pool server, so there's no need to reinstall pool to another machine. I'm covering all financial loss from my own money, to keep pool users out of this stupid issue.

Buy Trezor! | Slush Pool | SatoshiLabs

gratuitement des BTC, a été affecté par cet événement malheureux… Ah oui parce que si vous l'ignoreriez, il y a eu un moment dans l'histoire où des bitcoins étaient donnés gratuitement juste dans le but d'aider à développer la communauté et créer une économie saine.

Mais revenons au vol: sur les 50 000 bitcoins perdus ce jour-là, "seulement" 3094 appartenaient à Slush Pool, soit environ 15 312 dollars, le cours du bitcoin étant alors légèrement inférieur à la barre des 5 dollars à ce moment là. Réévalué à la date du 1er Novembre 2021, cette perte s'élève à près de 189 millions de dollars.

Slush décida de couvrir cette perte avec ses propres fonds, afin qu'aucun des participants de la pool ne soit affecté par ce regrettable événement. Cependant, tout cela lui servit de leçon – si dans les faits il avait perdu cet argent qui était le fruit de mois de travail pour Slush Pool, il pris alors la décision de tout mettre en en oeuvre pour qu'un tel incident ne se reproduise plus jamais.

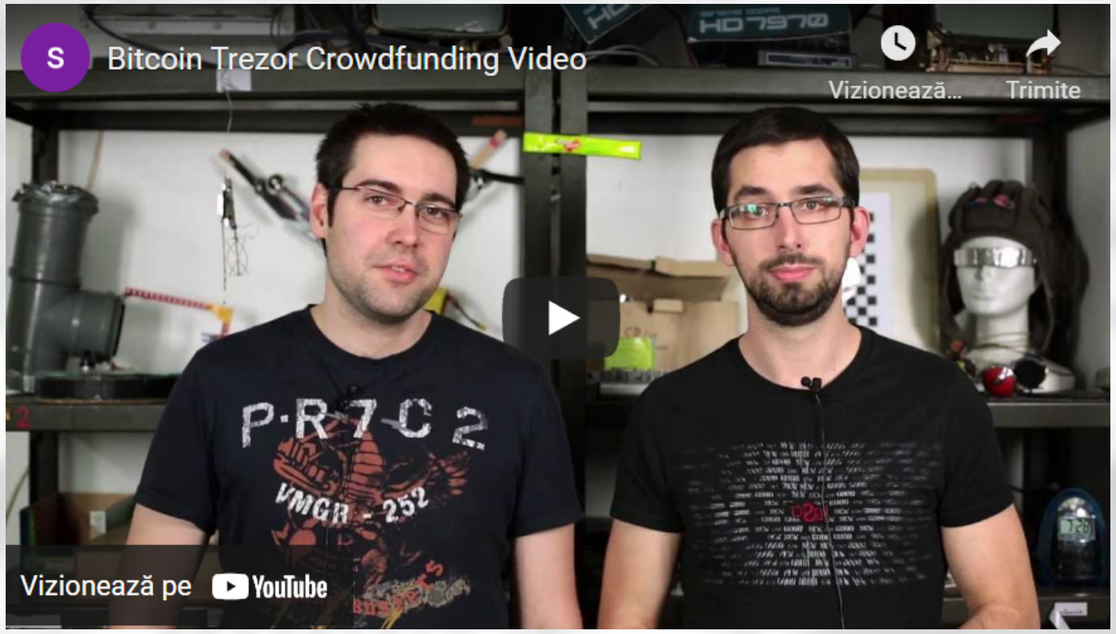
Le cypherpunk tchèque a rapidement compris que le problème ne concernait pas uniquement Linode : cette mésaventure aurait pu arriver à n'importe quel autre service connecté en permanence à Internet, et qui peut donc par conséquent être victime d'une attaque. Et comme l'intérêt pour Bitcoin ne cessait de croitre, il était indispensable de concevoir une meilleure solution pour la gestion des clés privées.

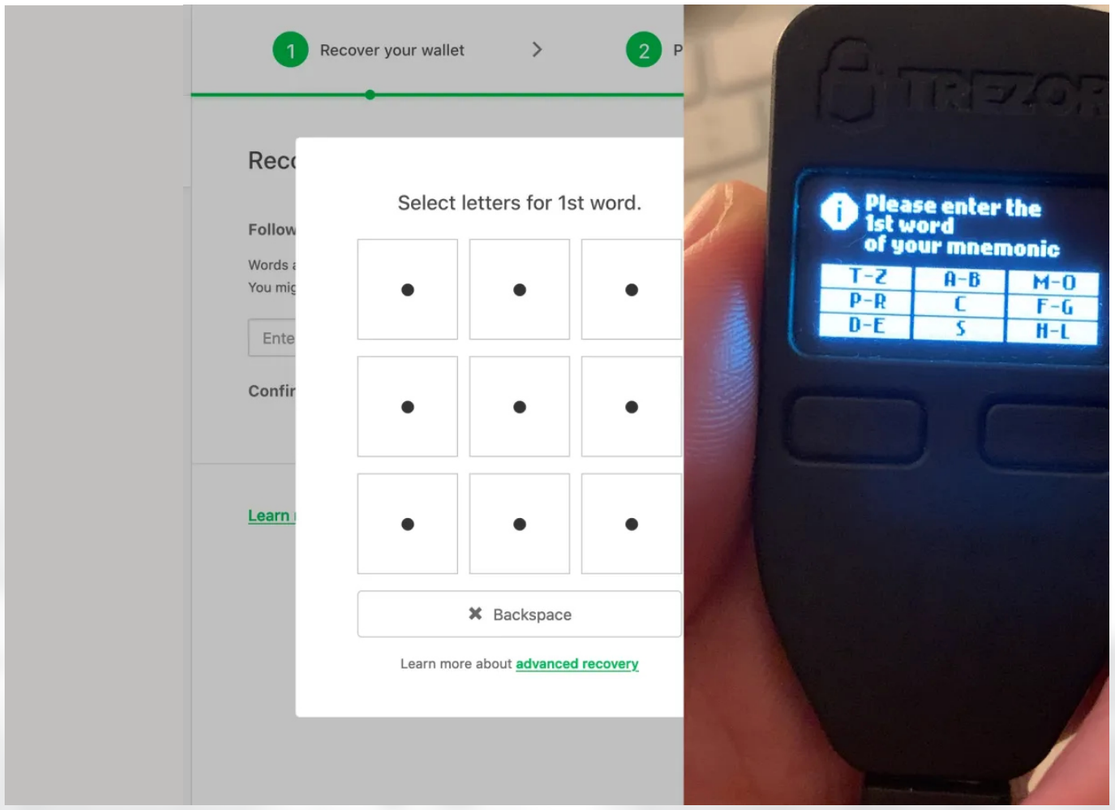
Et Le Monde Fit La Connaissance De Trezor: Le Premier Hardware Wallet Bitcoin

Après le hack des 3094 BTC, il aura fallu attendre deux ans et demi pour que les adeptes de sécurité Bitcoin puissent mettre la main sur Trezor. Et le prix de base du produit à l'époque s'avère déconcertant pour un bitcoiner d'aujourd'hui : 1 BTC (500 $ environ au moment de son lancement) pour la version standard avec boîtier plastique, et 3 BTC (1500 $ en mai 2014) pour la version avec boîtier métallique.

Pour leur défense, le prix du bitcoin est passé de 118 dollars en mai 2013 à 500 dollars en mai 2014, et a même ensuite dépassé la barre des 1000 dollars fin novembre. Ce n'était donc pas le moment idéal pour utiliser le BTC comme unité de compte (même s'il est vrai que le prix est resté aux alentours de 400 dollars pendant une majeure partie de 2014).

Le parcours qui a mené au lancement du premier hardware wallet au monde est loin





d'avoir été un long fleuve tranquille et constitue également à lui seul une sorte d'odyssée. – Slush a fait appel à deux amis afin de créer SatoshiLabs (le collaborateur de Slush Pool et créateur de CoinMap, Pavol "Stick" Rusnak, ainsi qu'une chargée de développement commerciale: Alena Vranova).

Bien qu'ils aient été confrontés à des problèmes aussi bien au niveau de la fabrication que de la distribution, leur apport à cette industrie a été vraiment monumental : un appareil qui gère vos clés privées dans un environnement sécurisé, qui est open source et vérifiable tout autant que peut l'être le code Bitcoin lui-même, et qui effectue des transactions si et seulement si vous appuyez sur un bouton physique qui fait office de confirmation.

C'est grace au Trezor que les standards BIP 39 et BIP 44 sont devenus si populaires – après sa sortie, de nombreux wallets ont adopté le format de cryptage à 12/24 mots mnémoniques et ont aussi ajouté le support du Bitcoin Testnet.

De plus, en raison de la nature open source du Trezor, de nombreux autres hardware wallet ont pu émerger et offrir sur le marché un panel de fonctionnalités supplémentaires présentant divers compromis : le KeepKey, le Coldcard, le BitBox, le Jade ou le Passport, doivent tous leur existence à la conception et au codebase du Trezor.

Et ce n'est pas comme si SatoshiLabs avait cessé d'innover après la sortie du Trezor. La société est à l'origine de la création de plus de 50 standards open source et contribue encore aujourd'hui à de nombreux autres repos open source (NixOS, Bitcoin Core, MicroPython, etc.).

Plus récemment, ils ont également décidé de se lancer dans la création de puces à éléments sécurisés véritablement transparentes avec l'entreprise Tropic Square (qui pourrait produire un nouveau hardware wallet Trezor fin 2022).



Les Bénéfices De Taproot En Matière De Confidentialité

Le soft fork Taproot est une étape essentielle pour améliorer la confidentialité on-chain de Bitcoin. Après l'activation de l'upgrade le 14 novembre 2021 à la hauteur de bloc 709632, les sociétés d'analyse de blockchain vont avoir plus de mal à déterminer ce qui se passe sur le public ledger. Comme un caillou dans la chaussure de ceux qui cherchent à désanonymiser toutes les transactions Bitcoin, Taproot fait en sorte que la plupart des contrats on-chain et des transferts conditionnels apparaissent identiques aux transferts ordinaires. Indirectement, ça favorise également la scalabilité (les configurations multisig ne nécessitent plus un block space supérieur) et les frais (des transactions plus petites se traduisent par des coûts moins élevés pour les utilisateurs).

Cet article, cependant, va uniquement se concentrer sur l'aspect vie privée du soft fork de Bitcoin. Il vise à éclaircir comment Taproot augmente le déni plausible de chaque utilisateur et constitue potentiellement une menace pour le secteur d'analyse de blockchains. Afin de rendre cette amélioration plus facile à comprendre, nous allons décomposer les avantages selon les différents cas d'utilisation.



Comment Taproot Améliore La Confidentialité Du Réseau Lightning

Le réseau Lightning est la couche de Bitcoin permettant d'effectuer des transactions quasi-instantanées, plutôt privées et très peu coûteuses. Contrairement à une blockchain, ce réseau est extrêmement évolutif, rapide et ne nécessite pas que l'ensemble du réseau stocke et valide chaque opération. Son élégante conception permet également une confidentialité plus élevée: seules les parties impliquées dans le transfert d'argent et les nœuds de routage sont en mesure d'obtenir des informations sur une transaction en cours. Les personnes extérieures sont complètement laissées dans l'ignorance et restent incapables d'évaluer quels acteurs sont engagés dans la transaction et quelle quantité de bitcoins a été déplacé.

Mais dans la mesure où Taproot est un upgrade de la base layer, affecte-t-il réellement Lightning ? Sans cet upgrade Schnorr-friendly, les ouvertures et fermetures de canaux sont dévoilés au niveau de la blockchain publique exactement pour ce qu'elles sont : des multi-sigs 2 sur 2 avec des contrats hashed time locked (HTLCs). Cependant, après l'activation de Taproot, toutes les entités ouvrant ou fermant un canal Lightning de manière collaborative apparaîtront comme effectuant une transaction ordinaire, et par conséquent indiscernables des autres transactions.

Auparavant, les analystes blockchain étaient capables de discerner quand certaines transactions servaient à fermer des canaux Lightning. Mais avec Taproot, ils peuvent uniquement constater que les coins ont bougé. Ils sont incapables de dire comment ces derniers ont bougé, et ne peuvent que constater que le montant a été dépensé d'une manière qu'il est impossible de distinguer.

Cependant, le niveau de confidentialité n'est toujours pas parfait. Comme l'a souligné Adam Ficsor, créateur de Wasabi Wallet, les canaux Lightning non privés diffusent un channel point qui correspond à l'output d'ouverture. Par conséquent, ce résidu d'information, qui peut être observé sur le réseau Lightning, procure également des informations sur l'output qui est engagée dans l'ouverture du canal. Taproot rend l'ouverture des canaux du réseau Lightning privée, mais seulement si les canaux sont privés également. Pareillement, même si une transaction CoinJoin avant et après l'ouverture d'un canal Lightning peut obscurcir l'avant et l'après, le "gossip" Lightning révèlerait toujours l'UTXO précis



contrôlé par l'opérateur du noeud. Des recherches prometteuses sont menées pour atténuer ce problème avec des ring-signature proofs pour la protection contre les dénis de service.

Comment Taproot Améliore La Confidentialité Sur Les Sidechains

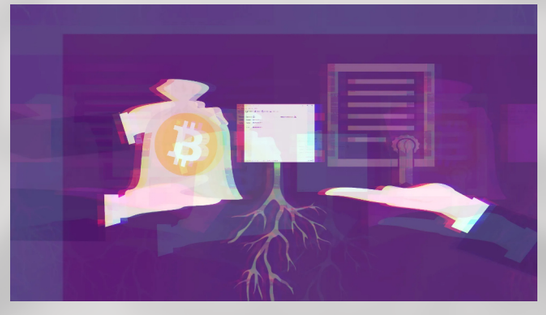
Tout comme les ouvertures de canaux Lightning, les peg-ins des sidechains reposent également sur un contrat multisig. Sur RSK par exemple (Rootstock, une sidechain Bitcoin qui vise le portage des smart contracts Ethereum), il y a un two-way peg (2WP) qui garantit que le BTC est transféré en toute sécurité. Mais avec Taproot, cette transaction ne se distingue pas de toutes les autres et occupe également moins d'espace dans les blocs.

Il en va de même pour la sidechain fédérée Liquid de Blockstream, ainsi que pour les Drivechains. Les transactions classique, les peg-ins de Liquid, les canaux Lightning et les multisigs des utilisateurs ont tous exactement la même apparence.

Comment Taproot Améliore La Confidentialité Des Multisigs

Ces dernières années, les configurations multisig sont devenues extrêmement populaires parmi les bitcoiners. L'expérience utilisateur s'étant améliorée avec des portefeuilles tels qu'Electrum, Sparrow ou Specter, de nombreux membres de la communauté ont choisi de rendre leurs bitcoins plus difficiles à voler, à pirater ou à dépenser. L'idée sous-jacente est que vous n'avez pas besoin de faire confiance à un seul portefeuille ou entité pour le caractère aléatoire et la sécurité de votre clé privée. Vous utilisez différents appareils dotés de différentes processing units pour générer vos clés, et vous pouvez ensuite aller jusqu'à distribuer vos sauvegardes de clés privées dans différentes parties du monde.

En fonction de votre configuration (la plupart des utilisateurs choisissent des 2 sur 3, mais vous pouvez aller jusqu'à 15 sur 15 si vous préférez la complexité), vous pouvez obtenir beaucoup de sécurité supplémentaire en sacrifiant la facilité de leur accessibilité. Par contre prenez garde à ne pas rendre le processus de récupération de vos bitcoins trop difficile, pour vous y compris, sinon vous risquez de perdre l'accès à ces derniers.



Taproot présente deux avantages essentiels pour les configurations multisig : il les rend plus accessibles (le coût de transaction pour signer une transaction 19 sur 20 sera le même que pour une simple transaction) et ajoute également une couche supplémentaire de confidentialité. Toutes les informations inutiles n'apparaîtront plus sur la blockchain publique. Cela préserve le secret de tous les signataires en n'affichant que l'entrée principale et sa sortie correspondante. Avant Taproot, une analyse de la blockchain pouvait permettre de déterminer quelles clés du setup avaient signé la transaction. Avec Taproot, cette information n'est plus publiquement disponible.

Comment Taproot Améliore La Confidentialité Des Smart Contracts Bitcoin

Depuis le tout premier jour, Bitcoin a permis l'utilisation de smarts contracts. Fondamentalement, les utilisateurs pouvaient déjà émettre des transactions conditionnelles indiquant au reste du réseau quand les fonds deviendraient disponibles pour être dépensés. Les configurations multisig, les ouvertures de canal Lightning et les peg-ins des sidechains sont autant de variations qui font appel à différents types de conditions.

Considérons donc un contrat de base dans lequel Alice verrouille ses bitcoins



jusqu'à une certaine hauteur de bloc, lorsqu'elle pense que son enfant Bob sera un adulte par exemple, ou bien permet à Bob d'accéder aux fonds dès qu'il devient techniquement capable de signer une transaction multisig. Jusqu'à Taproot, les deux conditions étaient révélées à l'ensemble du réseau et faisaient partie de l'immuable ledger. Mais avec Taproot, seule celle qui est exécutée devient publique. Il s'agit d'une amélioration de l'efficacité qui permet d'économiser un espace de bloc précieux, mais aussi d'un excellent moyen de protection de la vie privée qui permettra de mettre en place de nombreuses méthodes créatives afin de conserver de la richesse à travers le temps.

Taproot Simplifie Les Coin Swaps Invisibles

Mercury Wallet de CommerceBlock a vu sa popularité augmenter ces derniers mois. Ceci est dû à une fonctionnalité spéciale qui consiste à effectuer un changement de propriété de l'output sur le réseau Lightning et permet aux utilisateurs d'échanger efficacement l'historique des transactions de leurs coins d'une manière élégante et scalable. Si des bitcoiners ouvrent des canaux Lightning et s'échangent des UTXO entre eux, ils peuvent cacher une grande partie des activités précédentes impliquant leur argent et revenir sur la blockchain principale avec un set différent de coins. Mercury Wallet utilise le concept de statechains de Ruben Somsen pour verrouiller les fonds pendant une durée prédéterminée et effectuer des mélanges entre des outputs égaux.

D'une certaine manière, les Coinswaps sont des CoinJoins qui utilisent la scalabilité et les faibles frais de Lightning. Grâce à Taproot, ils sont également indiscernables des autres transactions.

Cependant, avec les Coinswaps, vous êtes toujours confronté au risque de recevoir un UTXO plus problématique qui peut avoir un passé "criminel". Au lieu de combiner plusieurs historiques de transactions (comme dans le cas des CoinJoins), il permet un marché anonyme de swaps d'historiques de transactions. Comme le créateur du portefeuille Wasabi, Adam Ficsor, l'a souligné dans une interview récente, les deux solutions de confidentialité peuvent devenir des outils complémentaires : "La combinaison des deux semble toutefois être la plus intéressante: CoinSwaps vers et à partir des CoinJoins, ce qui permettrait aux sets Coinjoins avec un anonymat limité d'obtenir autant de privacy qu'un CoinSwapper"

La Confidentialité Bitcoin Après Taproot

Avec Taproot, Bitcoin a subi un upgrade longtemps désiré vers l'utilisation des signatures Schnorr, plus efficaces, tout en faisant quelques pas de plus en direction de la victoire dans la lutte contre la surveillance financière. Ça ne signifie pas pour autant que l'analyse blockchain devient obsolète après cet upgrade. Tout d'abord, il faudra du temps aux utilisateurs pour mettre à jour leurs nœuds avec le dernier client adapté à Taproot (tout le monde ne peut donc pas encore profiter de ses avantages). Ensuite, les développeurs doivent mettre sur le marché des portefeuilles et des applications qui utilisent tout le potentiel de Taproot. Pour l'instant, peu de choses ont changé depuis le bloc 709632, lorsque le soft fork a été activé. Mais les nombreux avantages de Taproot peuvent laisser espérer une adoption rapide.

En outre, le protocole Bitcoin peut encore être optimisé pour la scalabilité et la confidentialité. L'une de ces optimisation pourrait être l'OP_CHECKTEMPLATEVERIFY (BIP 119, anciennement connu sous le nom d'OP_SECURETHEBAG) de Jeremy Rubin, qui regroupe les transactions pour réduire la quantité d'inputs et diminuer les frais pendant les moments de forte demande et de congestion. Grâce à elle, les CoinJoins et les Coinswaps peuvent bénéficier d'un déni encore plus plausible puisque la même technique devient une composante naturelle de la routine des transactions Bitcoin.

Parmi les autres solutions, citons Drivechains (Paul Sztorc a réussi à créer une chaîne type Zcash avec pour but d'augmenter la fongibilité des bitcoins traités), les extension blocs Mimble Wimble (une expérience en cours sur Litecoin, qui pourrait être utile si elle s'avère fonctionner), et l'espoir que les développeurs de Core trouveront un moyen d'intégrer les Zero-Knowledge proofs ou les Confidential Transactions sans nécessiter de hard fork. Cependant, ce Taproot reposant sur les signatures de Schnorr reste un excellent début et la manière dont il a été activé nous apporte l'espoir qu'un jour les bitcoins acquerront une fongibilité quasi absolue.



WASABI.WALLET 2.0
le portefeuille Bitcoin qui assure votre confidentialité par défaut
- Mélangez n'importe quel montant via CoinJoin
- Aucun frais de coordination en dessous de 0,01 BTC
- Aucun frais de coordination pour remixer directement depuis un mélange CoinJoin et pour la transaction suivante.
Wasabi Wallet – La référence en matière de confidentialité Bitcoin
wasabiwallet.io



CONSTRUIRE SOI-MÊME SON HARDWARE WALLET, PARTIE I : CONSTRUISEZ VOTRE TREZOR ONE, MODEL T ET BITBOX02

Construire Soi-Même Son Hardware Wallet, Partie I : Construisez Votre Trezor One, Model T Et BitBox02

Nous vivons l'âge d'or du bricolage DIY. Grâce aux progrès réalisés dans le domaine des microprocesseurs et de leur production/distribution, on peut aujourd'hui acheter des ordinateurs minuscules et pourtant assez puissants à des prix étonnamment abordables – et s'en servir pour effectuer des tâches étonnamment complexes.

La communauté Bitcoin s'en est clairement rendu compte et a transformé certaines de ces puces destinées à usage général en machines en petites machines de souveraineté financière. Des populaires puces ARM Cortex STM32 à l'étonnamment bon marché Raspberry Pi Zero, il existe de nombreuses options que vous pouvez utiliser pour construire votre propre hardware wallet. Mais avant de parler des options dont vous disposez pour construire ces derniers, il est important de mentionner les raisons pour lesquelles vous devriez embrasser cette solution.

Pourquoi Le Bricolage "Do It Yourself" Est-Il Préférable ?

Tout d'abord, il faut prendre en considération la situation de personnes vivant dans un pays dont la distribution de Trezor, Ledger ou BitBox02 est inexistante; dans ce cas construire son propre appareil est certainement l'option la plus abordable. Deuxièmement, si votre gouvernement est hostile au Bitcoin et à tout ce qui le concerne, alors c'est également fortement recommandé d'utiliser les mêmes composants que ceux pouvant par exemple être utilisés pour construire un petit appareil portable pour jouer à Tetris afin de sécuriser votre précieux or numérique.

Et même si vous vivez dans un pays où la distribution des hardware wallets commerciaux est possible, vous devriez envisager la voie du bricolage DIY. Si vous



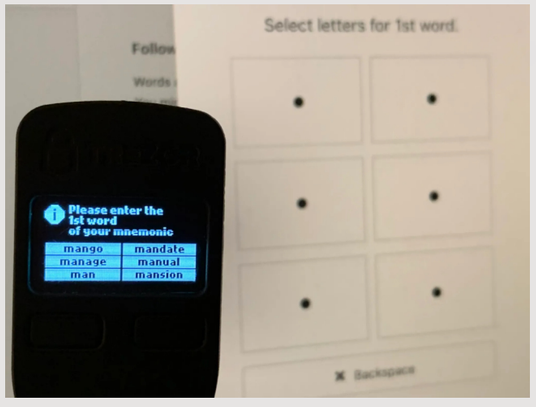
vous préoccupez réellement de la protection de votre vie privée (et ça devrait clairement être le cas), vous ne devriez pas donner votre nom et votre adresse à un vendeur ou à une société de livraison qui conserveront vos données dans leurs archives pendant plusieurs années – le cas du hack de la base de données Ledger est un très bon exemple de l'importance de la protection de la vie privée et de l'avantage apporté par du matos bricolé en DIY.

En outre, les risques d'attaque au niveau de la chaîne d'approvisionnement sont réels : vous ne savez pas qui va manipuler votre hardware wallet à partir du moment où il quitte l'usine jusqu'à ce qu'il vous soit finalement livré. Si un livreur sait ce qu'est un Trezor, il peut compromettre son matériel ou son emballage (une attaque très populaire implique l'insertion de seed phrases BIP 39 déjà générées, dans l'espoir que les nouveaux venus déposent leurs coins à des adresses contrôlées par l'acteur malveillant).

Bien sûr, les sociétés font de gros efforts pour empêcher de telles attaques en superposant plusieurs couches de protections pour leurs emballages et en introduisant des astuces cryptographiques pour vérifier l'intégrité du matériel et du logiciel. Mais si vous avez un minimum de maitrise, le bricolage DIY est définitivement plus sûr: l'utilisation d'un matériel polyvalent disponible sur le marché et d'un logiciel libre que vous pouvez personnellement vérifier est définitivement l'approche conseillée pour un utilisateur expérimenté.

Les Hardware Wallets Que Vous Pouvez Construire Vous-Même :

Il est donc temps maintenant de considérer les hardware wallets que vous pouvez construire vous-même. Il se divisent essentiellement en deux catégories : les appareils commerciaux dont les circuits et les schémas ont été mis en libre accès et les projets communautaires à but non lucratif qui ont été conçus spécifiquement pour le bricolage DIY. Le Trezor et le BitBox02, qui font partie de la première catégorie, ont l'avantage d'avoir un codebase et une architecture bien plus testées et scrupuleusement examinées puisqu'ils sont vendus dans le commerce. Les équipes à l'origine de ces projets peuvent se permettre de payer des bounties et des audits de sécurité, mais d'un autre côté les pirates sont également plus enclins à les "casser".



D'un autre côté, les projets complètement DIY comme SeedSigner, Specter DIY ou Bowser offrent un niveau de facilité supplémentaire, car ils peuvent être construits à partir de composants très courants et ne nécessitent quasiment aucune soudure ou expérience en électronique. Ils ne sont pas aussi éprouvés que leurs homologues commerciaux et vous pouvez difficilement vous attendre à recevoir autant de soutien dans le processus. Pourtant, ils présentent des avantages qui leur sont propres et donnent à chacun la possibilité de devenir financièrement souverain.

Commençons tout d'abord par analyser ce qui est nécessaire afin de construire votre propre Trezor et/ou BitBox02. Ensuite, la seconde partie se concentrera sur le Seedsigner, le Specter DIY, et le Bowser wallet.

Construire Son Propre Trezor One :

Lors de la campagne Kickstarter de 2014 qui a conduit au lancement du premier hardware wallet Bitcoin, les cofondateurs de Trezor, Marek "Slush" Palatinus et Pavol "Stick" Rusnak, ont affiché leur intention de créer un appareil qui pourrait satisfaire jusqu'aux exigences du créateur de Bitcoin, Satoshi Nakamoto lui même. Ça signifie concrètement que le logiciel et toute la circuiterie sont transparents et 100% open source, de sorte que tout le monde puisse voir ce que fait l'appareil à tout moment.

Le repository GitHub de la société tchèque propose le circuit imprimé complet, les schémas et la la nomenclature (BOM). Selon ces documents, vous avez besoin de 24



composants différents, les plus importantes étant l'écran OLED, le microcontrôleur STM32F10XRXT6, les boutons, le boîtier, le commutateur tactile et le port micro-USB. Le coût de l'ensemble ne devrait pas dépasser 20€, mais vous devez également disposer d'un fer à souder et de la dextérité nécessaire pour assembler le tout par vous-même.

En toute objectivité, même si le coût de production d'un hardware wallet Trezor One est faible, la partie assemblage peut s'avérer difficile et intimidante pour un débutant. Clairement, notez que si vous choisissez de construire vous-même le hardware wallet le plus éprouvé au monde, vous allez devoir développer quelques compétences pratiques. Ce n'est pas surprenant en fait que le Trezor One soit l'appareil le plus copié du marché et qu'il existe des centaines d'entreprises qui le vendent sous différentes marques partout sur la planète. En fait, des appareils plus récents tels que BitBox02, Coldcard et le Passport de la société Foundation utilisent des parties importantes du code du Trezor et, dans une certaine mesure, peuvent être qualifiés de "clones".

Dès que vous aurez fini d'assembler votre Trezor One personnalisé, vous pourrez flasher le firmware en suivant les instructions du depository GitHub. Une fois ceci accompli, votre nouveau hardware wallet fonctionnera parfaitement avec la plupart des wallet du marché si vous choisissez de ne pas opter pour Trezor Suite.

Pour plus d'informations sur l'éthique et l'engagement open source de Trezor, vous pouvez écouter l'entretien avec le PDG Marek "Slush" Palatinus sur le podcast de Bitcoin Takeover S4E8.

Construire Son Propre Trezor Model T :

Lancé à l'automne 2017, la deuxième génération de hardware wallet Trezor comporte des améliorations indispensables. Il remplace le panneau à deux boutons précédent par un écran tactile couleur plus facile à utiliser, et il est également doté d'un processeur plus rapide qui permet de réaliser des sauvegardes plus complexes, comme le partage de clés secrètes de Shamir. L'appareil est également plus fiable pour gérer les configurations multisig complexes (telles qu'un 8 sur 8 par exemple), comme cela a été démontré par Jameson Lopp dans l'une de ses études comparatives.

Cependant, le Trezor Model T est doté d'une bien grande complexité électronique : la nomenclature (BOM) énumère 109 composants, en même temps que les circuits imprimés sont bien plus élaborés et sophistiqués. Cela signifie que le Trezor Model T est un projet de bricolage largement plus difficile et plus exigeant que son prédécesseur. Pour compenser tout ça, les instructions de montage sont également bien plus détaillées et comportent davantage de photos pour vous guider à chacune des étapes.



En termes de sécurité, le modèle T présente l'avantage de vous permettre de taper votre passphrase directement depuis votre appareil, ce qui est une fonctionnalité intéressante, surtout si vous suspectez le clavier de votre ordinateur d'être potentiellement compromis/enregistré. Donc, même si vous ne vous souciez pas beaucoup des options multisig ou des sauvegardes Shamir, ça vaut tout de même la peine de considérer le Modèle T pour son upgrade au niveau de la saisie.

La puce qui pilote le Trezor Model T est le microcontrôleur STM32F427VIT6, une unité ARM Cortex M4 dotée de 2 mégaoctets de mémoire flash et cadencée à 168 Mhz. Vous pouvez la trouver pour environ 20€, mais vous obtiendrez certainement de meilleurs deals si vous en achetez plusieurs à la fois. L'écran coûte pour sa part environ 5€, et le reste de l'électronique devrait ajouter à la note encore 20€ supplémentaires (du boîtier aux ports USB-C et micro-SD, jusqu'aux divers connecteurs). Mais avant de juger Trezor pour avoir vendu son appareil à un prix qui dépasse largement ses coûts de production, il ne faut pas oublier que la fabrication de cet appareil nécessite des compétences avancées en matière de soudure (bien supérieures à celles nécessaires pour le Trezor One), que la société se concentre principalement sur l'amélioration des normes de sécurité logicielle (vous payez donc pour la recherche et le développement des SLIPs) et qu'une partie du prix est liée au support client offert par Trezor.

Pour un bricoleur expérimenté, le modèle Trezor T peut être un projet amusant pour vous occuper le week-end. Le fait que les composants soient des pièces communes et faciles à trouver en ligne devrait fournir une forte quantité de déni plausible si vous résidez dans un état autoritaire, et les caractéristiques supplémentaires feront que l'effort supplémentaire en vaudra la peine (par rapport au Trezor One plus simple).

Tout comme le Trezor One, vous pouvez utiliser votre Model T nouvellement construit avec une multitude de wallets disponibles sur le marché. Gardez à l'esprit cependant que certains d'entre eux ne fonctionneront pas avec les configurations multisig et le partage de clé secrète Shamir. Seules les configurations BIP39 seront effectives.

Construire Son Propre BitBox02 :

Lancé à l'automne 2019, le BitBox02 est une variation du design original du Trezor qui apporte plusieurs modifications matérielles et logicielles substancielles. Bien que le produit s'appuye sur la même codebase de départ, il est suffisamment différent pour mériter qu'on le mette en avant. D'un point de vue philosophique, le dispositif vise à offrir le compromis entre l'auditabilité de l'open source et la sécurité physique, ce qui le place dans une position intermédiaire entre Trezor (100% open source) et Ledger (environ 40% open source, et avec sa puce de sécurisation qui reste opaque).

La partie qui rend le BitBox02 moins open source que le Trezor mais plus sûr physiquement c'est l'utilisation de la puce de sécurisation plus générale ATECC608B. Ça signifie que vous pouvez empêcher un accès physique d'un acteur malveillant à votre appareil sans avoir recours à une passphrase logicielle (que vous pouvez potentiellement oublier ou perdre si vous n'êtes pas assez prudent). Donc, si vous voulez faire passer votre sécurité physique au niveau supérieur, vous devriez envisager de construire un BitBox02.

Outre la puce de sécurisation, cette deuxième génération de hardware wallets produits par ShiftCrypto nous gratifie de plusieurs choix intéressants : l'appareil utilise un connecteur USB-C mâle qui permet de le brancher facilement sur votre téléphone portable (aucun câble n'est nécessaire tant

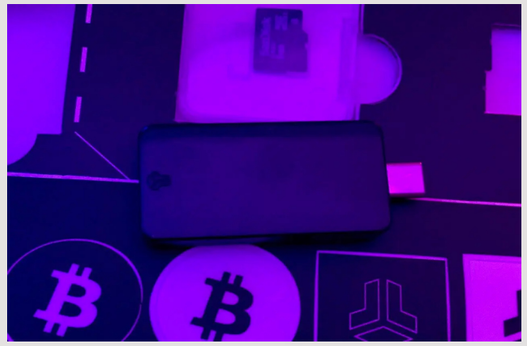
que vous disposez du bon port sur votre ordinateur ou votre téléphone), et l'écran tactile est remplacé par des capteurs tactiles sur le dessus et le dessous du hardware wallet.



En termes de logiciel, le BitBox02 utilise les signatures de Schnorr pour vérifier l'intégrité du logiciel et empêcher les attaques de la chaîne d'approvisionnement. Ce système est appelé anti-klepto et, même s'il ne semble pas forcément très pertinent pour quelqu'un qui construit lui même son propre hardware wallet, il s'agit d'un excellent outil d'auto-vérification qui empêche toute intervention extérieure sur le code. Pour en savoir plus sur ce mécanisme de sécurité, vous pouvez écouter l'interview de Benma, chercheur et développeur de logiciel chez ShiftCrypto (BTCTKVR S8E2).

Pour vous aider à construire votre propre BitBox02, ShiftCrypto a publié une nomenclature (BOM qui devrait être mise à jour pour inclure la puce ATECC608B qui a remplacé la 608A en 2021), une fiche technique détaillée, les schémas du circuit imprimé et même une photo aux rayons X qui devrait vous aider à comprendre comment connecter chaque composant au circuit. Le guide n'est pas aussi détaillé que dans le cas des hardware wallet Trezor, mais tout amateur un peu expérimenté devrait être en mesure de le comprendre.

Parlons maintenant des coûts : en gros, la puce sécurisée ATECC608B peut être achetée pour environ 1€. Mais en raison de problèmes d'approvisionnement dans l'industrie des micropuces, elle semble actuellement être en rupture de stock sur certains sites de vente en ligne les plus populaires (et entrainant ainsi surement une



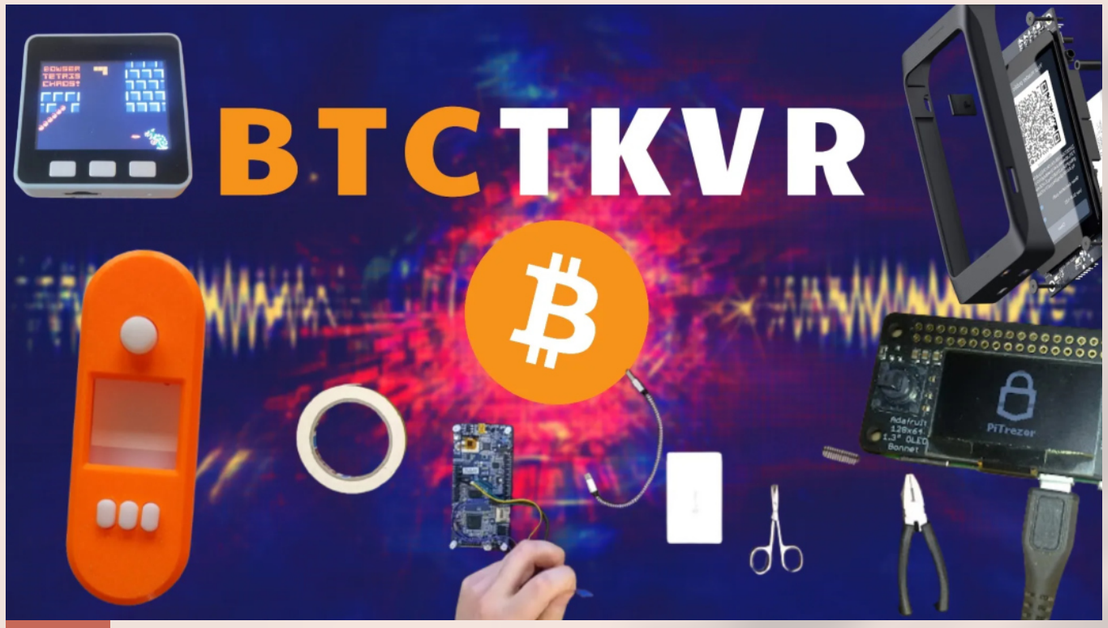
hausse de son prix en raison de sa rareté). D'autre part, la puce microcontrôleur 32 bits ARM Cortex M4F ATSAMD51J20A coûte environ 6€ et semble également difficile à trouver. Les diodes de suppression PRTR5V0U2F et tous les autres petits composants ajoutent également environ 3€ au coût de production. Au total, l'achat des pièces nécessaires à la construction de votre propre BitBox02 devrait coûter environ 20€ (inclus le port USB-C, le logement pour carte micro-SD, les capteurs tactiles et l'écran OLED).

Le BitBox02 comporte plus de composants que le Trezor One, mais moins que le Trezor Model T. Il comporte également des composants plus abordables que le modèle phare de Trezor et offre une certaine sécurité physique. Donc si vous recherchez ces caractéristiques, vous devriez dès à présent empoigner votre fer à souder et commencer à commander les composants pendant qu'ils sont encore en stock.

La Construction De Votre Hardware Wallet Doit-Elle Être Nécessairement Aussi Difficile ?

Eh bien, non. Aujourd'hui, nous avons les appareils SeedSigner, Specter DIY et Bowser et ils sont beaucoup plus accessibles aux amateurs qui ne veulent pas souder des diodes sur un PCB tout en consultant des schémas complexes. Cependant, ils ne sont pas aussi testés que les appareils commerciaux, et c'est donc toujours une histoire de compromis. L'article suivant vous en dira plus sur la façon dont vous pouvez construire ces hardware wallet et sur les coûts que ça implique !





Construire Soi-Même Son Hardware Wallet, Partie II

Les Hardware Wallets Que Vous Pouvez Construire Vous-Même :

Il existe deux principales catégories de hardware wallets que vous pouvez construire à partir de composants électroniques d'usage général : ceux qui exécutent un firmware porté (un groupe de codeurs rend disponible un logiciel déjà bien éprouvé pour un hardware plus commun), et ceux qui exécutent un code original.

Tous deux sont assez faciles à construire en théorie et nécessitent d'assembler assez peu de composants. Mais dès le départ, vous devez comprendre les compromis inhérents à ces deux options: un projet comme PiTrezor peut être un portage pratique qui vous permet d'exécuter le logiciel du hardware wallet le plus éprouvé sur un Raspberry Pi, mais cela ne signifie pas pour autant que le portage lui-même est vérifié par des professionnels de la sécurité ou maintenu pour y inclure les dernières mises à jour de Trezor. À l'inverse, des projets comme SeedSigner ou Specter DIY peuvent être original et open source, mais cela n'implique pas forcément non plus que de nombreux experts aient vérifié leur code.

C'est pourquoi, concernant ces dispositifs que vous pouvez construire vous-même une des recommandation est la suivante: si vous en avez la capacité vérifiez le code ou bien de payez un professionnel pour le faire à votre place. De plus, si vous comptez utiliser ces hardware wallets faits maison pour protéger de grandes quantités de bitcoins, alors il est préférable d'opter pour une configuration multisig. Si chaque appareil n'est rien d'autre qu'une clé permettant d'accéder à vos coins et qu'il n'y a aucun point de défaillance unique pouvant vous faire perdre vos fonds, alors on peut considérer comme plus sûr d'utiliser ces appareils présentant potentiellement un niveau de risque plus



élevé.

À ce stade, on pourrait se poser une questions primordiale : pourquoi se bricoler un hardware wallet DIY si la sécurité pourrait éventuellement s'avérer douteuse? Eh bien, les deux meilleurs arguments pour répondre à cette interrogation sont les suivants: capacité à contourner un autoritarisme politique et défense contre les attaques possible de la chaîne d'approvisionnement. Une chose que vous construisez vous-même à partir de composants répandus va vous aider à préserver votre vie privée et votre déni plausible vis-à-vis de votre gouvernement – et la société de livraison n'aura également aucune idée de ce que vous faites.

Une fois encore, ces hardware wallets open source réalisables à la maison sont encore dans une phase précoce de leur développement et sont principalement recommandés pour les configurations multisig. Ne prenez pas de risques inconsidérés avec vos bitcoins. Si vous êtes un bricoleur amateur de hardware wallet ou un individu qui essaie d'acquérir sa souveraineté financière dans un environnement autoritaire, envisagez de créer des configurations plus élaborées qui ne reposent pas trop sur un seul dispositif – même si cela implique faire une sauvegarde Shamir ou une configuration multisig qui ne serait pas compatible avec certains logiciels du marché.

Après avoir exposé ces mises en gardes, examinons en détails les quatre hardwares wallets dans leur version bricolage DYI afin de déterminer les coûts, la difficulté et la complexité de la tâche à accomplir.

Construire Son Propre PiTrezor :

En matière de sécurité, une des règles de base est celle qui consiste à suivre la voie la plus éprouvée. De cette manière, vous avez plus de recul grâce aux expériences des autres et vous avez une meilleure compréhension de tous les compromis qui sont impliqués. Or puisque Trezor existe depuis 2014 et que son code a fait l'objet d'un examen constant depuis sa création, il est relativement sûr de supposer que le firmware fonctionne très bien et qu'il a été constamment endurci au fil des problèmes mis à jour.

PiTrezor est un portage du code original, qui fait fonctionner le firmware optimisé pour le STM32F10XRXT6 sur le Raspberry Pi Zero, plus répandu et plus populaire. Vous pouvez acheter un Pi pour pratiquement tout, de l'émulation de jeux vidéo à

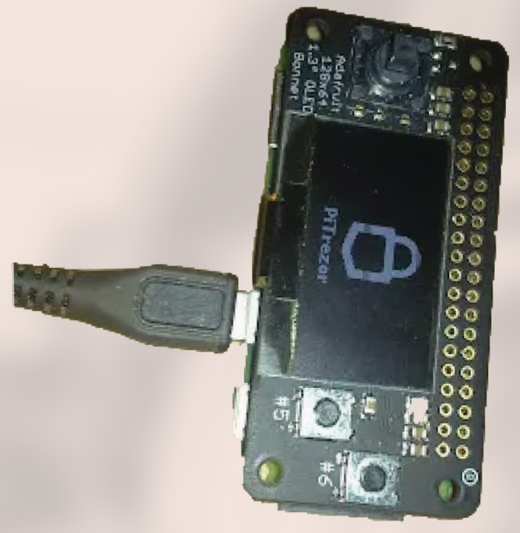
l'expérimentation IoT, en passant par la robotique et les relais Tor. De plus, le Raspberry Pi Zero ne coûte que 5€ et fait partie des mini-ordinateurs les plus accessibles, tant en termes de prix que de disponibilité aux quatre coins du monde. Si on le compare au microcontrôleur Trezor par défaut, le Pi Zero est bien plus populaire et par conséquent il s'avère bien plus facile de se procurer des accessoires compatibles avec celui-ci.



En outre, le portage PiTrezor fonctionne également sur le Raspberry Pi 4 – dispositif plus puissant qui est très souvent utilisé par les opérateurs de nœuds Bitcoin à leur domicile. Le principal avantage de ces appareils dans le cas présent, c'est qu'ils sont équipés de ports USB, ce qui vous permet de connecter votre clavier pour l'utiliser comme source d'entrée. Ça signifie concrètement qu'il n'est pas nécessaire de se soucier à trouver des boutons qui s'adaptent à tel ou tel sorte de boîtier, car vous avez simplement la possibilité de faire fonctionner le PiTrezor avec un périphérique que vous possédez déjà.

Par conséquent, le processus est beaucoup plus facile et ne nécessite aucune soudure ou d'assemblage d'éléments si vous choisissez de faire tourner PiTrezor sur un Raspberry Pi 4. Toutefois, il faut garder à l'esprit qu'il y a un surcout d'environ 30€ si vous optez pour cette configuration. Afin consulter le guide complet du projet, rendez-vous sur le site Web de PiTrezor.

Allez, parlons maintenant des composants et de leurs coûts. Il existe deux versions du Raspberry Pi Zero, et vous devriez prendre la version la plus basique et la moins onéreuse qui ne possède ni Bluetooth ni WiFi. Non seulement parce que ces ports sont inutiles, mais aussi parce qu'ils peuvent représenter des vecteurs d'attaque potentiels supplémentaires pour compromettre l'appareil ou extraire des informations. Bien que le responsable de PiTrezor suggère que le Zero W est tout aussi sûr dans la mesure où le firmware n'a pas de drivers chargés pour les ports de communication, un pirate compétent peut toujours les exploiter s'il arrive à avoir un accès physique à l'appareil . Par conséquent, pour des raisons à la fois de sécurité et d'économie, il est préférable d'acheter le Pi Zero de base à 5€.



Les autres composants comprennent une carte SD de plus de 100 Mo (en gros, n'importe laquelle que vous dégotterez pour quelques euros fera l'affaire), un câble micro-USB vers USB (environ 1€), un câble mini HDMI permettant de se connecter à un moniteur, une télévision ou un écran dédié (comptez environ 3€ en partant du principe que vous possédez déjà un moniteur ou une télévision), deux boutons-poussoirs compatibles avec le Raspberry Pi (environ 2€, et notez qu'ils ne sont nécessaires que pour la configuration du Pi Zero, dans la mesure où il est possible d'utiliser votre clavier USB avec le Pi 4) et des fils pour souder les boutons à la carte (environ 1€). Les composants optionnels comprennent un écran dédié, utile pour des raisons de portabilité, et un boîtier efficace pour protéger la carte et les circuits de la poussière, des dommages physiques et d'autres facteurs imprévus.

En supposant que vous allez payer 5€ pour le Raspberry Pi Zero et 9 à 10€ supplémentaires pour les autres composants, on peut évaluer que la construction de la version la plus basique mais assez exigeante sur le plan électronique du PiTrezor vous reviendra environ à 15€. Gardez toutefois à l'esprit que l'écran, le boîtier, le fer à souder et l'expédition de toutes ces pièces ne sont pas pris en compte et peuvent facilement doubler les coûts.

Si vous optez pour la configuration avec le Raspberry Pi 4, vous n'aurez besoin que de l'appareil à 35€ (choisissez le modèle d'entrée de gamme de 2 Go, vous n'aurez même pas besoin d'autant de mémoire pour un Trezor), de la carte SD à 2€ et des câbles micro-USB vers USB et mini-HDMI mâle vers HDMI femelle. Ces derniers devraient vous revenir à 6€ environ. Et si le total approximatif de 41€ peut sembler assez cher, au moins considérez que vous n'avez besoin de faire aucune soudure et que par conséquent aucun équipement spécial nécessaire à cette tâche n'est requis. Vous flashez le firmware sur la carte SD, branchez le Raspberry Pi sur une prise de courant, connectez le port vidéo externe à votre écran de télévision ou moniteur compatible HDMI (en gros tout écran de moins de 10 ans en est équipé), et utilisez votre clavier USB comme source d'entrée. C'est assez geek, mais quelqu'un qui vit dans un endroit où les hardware wallets Trezor ne sont pas distribués officiellement va forcément apprécier le niveau de souveraineté que peut apporter ce bricolage DIY.



Avant de passer à la partie suivante, voici un autre rappel qu'il est bon de faire: bien que le code du PiTrezor soit open source et qu'il s'agisse essentiellement d'un portage de la version officielle du Trezor, vous devez être extrêmement prudent et éviter de mettre trop de coins dans cet appareil sans avoir vérifié correctement le code au préalable. La façon la plus sûre d'utiliser un PiTrezor est d'en faire un de vos appareils multisig, afin d'éviter de présenter de point de défaillance unique. Mais vous devez toujours être prudent, comme l'a dit Marek "Slush" Palatinus, PDG de Trezor, dans le podcast S4E8 de Bitcoin Takeover, il existe a environ 40 clones de Trezor dans le monde et les modifications apportées à leur code n'est pas toujours examiné comme il le devrait.

Construire Son Propre Specter :

Le créateur de Specter, Stepan Snigirev, a instauré une véritable révolution dans le domaine des hardware wallets Bitcoin. Grâce à ses projets micro-bitcoin et micro-arduino, des appareils de faible puissance sont désormais capables d'exécuter une version légère du client Bitcoin. Plus remarquable encore, il a créé un hardware wallet qui peut être construit à partir de composants standard et qui exécute un code qui n'est pas celui de Trezor. Alors que tous les dispositifs électroniques de gestion de clés sécurisées disponibles dans le commerce, de KeepKey à Coldcard en passant par les Foundation Devices Passports, utilisent d'une manière ou d'une autre le firmware open-source de Trezor, le Specter DIY à l'audace d'être différent.



Pour construire votre propre Specter DIY, vous n'avez besoin que d'une developper board STM32F469I-DISCO que vous pouvez acheter pour environ 60€, ainsi que d'un câble mini USB et d'un câble micro USB à 1€ (que vous avez très probablement déjà pour

votre téléphones ou un autre hardware wallet). L'appareil lui-même possède tout ce dont vous avez besoin, de l'écran tactile à la mémoire flash que vous utilisez pour installer le firmware Specter. Il s'agit donc d'une solution tout-en-un qui, au pire, ne nécessite qu'un boîtier additionnel pour protéger de la poussière.

Aujourd'hui, de nombreux utilisateurs Bitcoin construisent leur propre hardware wallet Specter DIY afin d'éviter les attaques de la chaîne d'approvisionnement. Mais comme le code n'est pas autant vérifié que celui de Trezor et qu'il pourrait présenter des vulnérabilités qui n'ont pas encore été décelées jusqu'à présent en raison d'un manque d'incitations financière (le Specter DIY est encore un produit de niche difficile à trouver et la récompense pour craquer le code n'est en aucun cas comparable au programme de bounties de Trezor), il est préférable de garder le dispositif pour une configuration multisig. C'est exactement ce que recommandent les développeurs de Specter d'ailleurs: ils considèrent leur projet de bricolage DIY comme un complément aux autres hardware wallets. Vous pouvez certes l'utiliser comme un dispositif de single-sig, mais le cas d'utilisation où il se démarque le plus reste le multisig.

Pour le Specter DIY, il est également recommandé d'acheter un module supplémentaire qui permet de scanner les codes-barres qui coûte environ 40€. Il rendra l'appareil plus pratique d'utilisation, car vous pourrez scanner des QR codes et confirmer des transactions sans avoir à connecter votre appareil à un ordinateur. En outre, vous pouvez rendre le Specter DIY autonome le munissant d'une batterie. Les instructions de montage complètes sont disponibles dans le repository GitHub du projet. De plus, vous trouverez aussi un tutoriel vidéo assez détaillé sur YouTube.

Au total, la construction du Specter DIY devrait vous coûter entre 64 et 120 euros. Et si vous voulez aussi un boîtier, vous pouvez soit l'imprimer en 3D selon les spécifications, soit l'acheter auprès d'un professionnel ou amateur qui propose ce service. Cela peut certes donner l'impression que le Specter est un appareil onéreux, mais si vous l'achetez prêt à l'emploi, il vous en coûtera 350€ pour un boîtier complet, et 60€ pour avoir également la carte STM32F-469I-DISCO. Il est donc nettement préférable de débourser 150€ pour un dispositif complet que vous construisez vous-même à partir de composants provenant de différents fournisseurs que de dépenser 410€ pour le Specter Shield.



Pour mieux comprendre la portée et le but du projet Specter DIY, vous pouvez écouter Stepan Snigirev donner toutes les explications dans le podcast S8E11 de Bitcoin Takeover.

Construire Son Propre Seedsigner :

Le SeedSigner est un projet simplifié mais fortement inspiré du Specter DIY, qui remplace l'expérience de l'écran tactile par l'efficacité imparable de l'abordable Raspberry Pi Zero. Son objectif principal est d'offrir un dispositif puissant que tout le monde puisse construire pour environ 50€.

Contrairement au Specter DIY, le SeedSigner utilise une configuration plus traditionnelle avec ses boutons physiques. Le principal inconvénient de cette conception c'est que quelques points de soudure sont nécessaires pour assembler l'appareil. Toutefois, comme il s'appuie sur l'architecture du populaire Raspberry Pi, on peut facilement choisir d'acquérir des hamer headers GPIO (qui coûtent 7€) pour pallier à ce tracas, si c'en est un.

Pour assembler votre SeedSigner, vous avez donc besoin d'un nano-ordinateur Raspberry Pi Zero (une fois encore, la version de base à 5€ sans le Wifi et le Bluetooth est recommandée), d'un écran LCD carré de 1,3 pouce avec une résolution de 240×240 pixels (qui coûte environ 15€) et d'un appareil photo compatible avec le système Pi Zero (le modèle préconisé est le AuviPal 5MP 1080p, qui est actuellement en rupture de stock mais coûte habituellement environ 20€).



Le développeur principal de SeedSigner a également mis en open source les spécifications du boîtier, afin que toute personne disposant d'une imprimante 3D puisse créer le sien. C'est pas forcément positif pour ceux qui n'ont pas accès à une imprimante 3D, notamment en raison du fait que des boutons physiques qui sont un des éléments de ce boitier sont nécessaires pour la saisie. Cependant, il existe plusieurs vendeurs pro ou même des amateurs qui peuvent imprimer ces boîtiers pour vous pour quelques Euros.

Ainsi, si les composants électroniques nécessaires à la construction d'un SeedSigner coûtent environ 40€ (soit moins que l'objectif annoncé de 50€), il vous faudra dépenser un peu plus pour profiter de "la totale". Toutefois, il faut noter que la partie assemblage du SeedSigner est bien plus abordable pour un néophyte que celle du Specter DIY dont il emprunte le code.

En parlant du code, une fois que vous aurez assemblé le matériel, vous aurez besoin d'une carte SD et vous devrez également taper quelques commandes sur un clavier externe. Le guide complet disponible en ligne est relativement simple à suivre, de sorte que même si vous ne comprenez pas ce que vous faites, vous réussirez à configurer votre SeedSigner.

Vous devez également garder à l'esprit que le SeedSigner est un dispositif air-gapped qui est optimisé pour fonctionner avec des wallet compatibles multisig, tels que Specter Desktop, Sparrow ou BlueWallet. Vous pourrez y accéder uniquement à partir de wallets qui prennent en charge les configurations PSBT (Partially Signed Bitcoin Transaction). Pour le moment, il s'agit toujours d'un projet de bricolage geek que les utilisateurs occasionnels ne trouveront pas forcément très convivial ou accessible. Mais grâce aux contributions de sa communauté de passionnés, il a tendance s'améliorer très rapidement.



Pour mieux comprendre la philosophie derrière le SeedSigner, vous pouvez écouter le podcast S8E10 de Bitcoin Takeover. Si vous avez besoin d'aide en cours de route, vous pouvez utiliser le guide de montage complet disponible sur YouTube.

Construire Son Propre Bowser Wallet :

Créé par Ben Arc, le Bowser wallet est une version encore plus simplifiée du Specter DIY.

Tout ce que vous avez à faire pour construire ce hardware wallet est d'acheter un M5Stack ESP32 Basic Core à 40€ et d'installer le firmware via une carte micro-SD.

Cela signifie que le Bowser wallet est de loin le hardwarware wallet à bricoler soi-

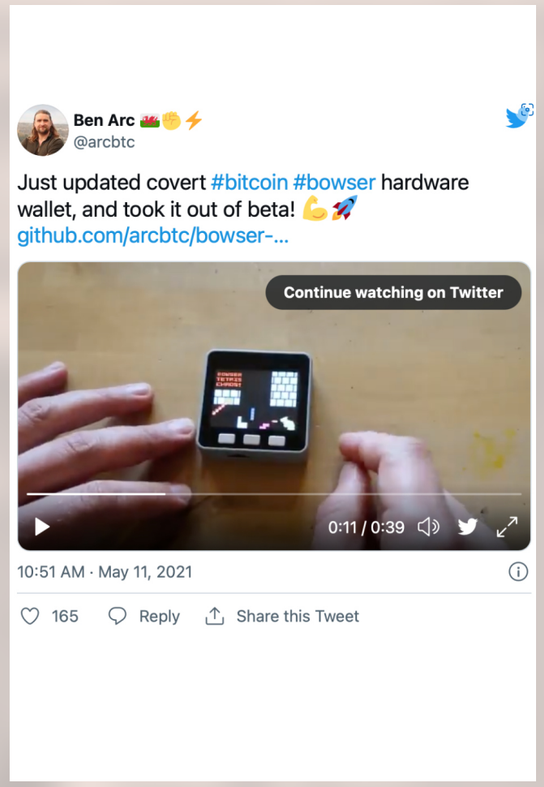
même le moins cher et le plus simple à configurer. Vous disposez même d'un guide complet sur YouTube qui vous aide, étape par étape, tout au long de la construction.

Cependant, il y a quelques bizarreries que vous devez prendre en compte : tout d'abord, ce hardware wallet fonctionne également comme un système de jeu vidéo qui exécute une version stylisée de Tetris.

Cela permet un déni plausible, car personne ne devinera que l'appareil d'apparence générique que vous tenez dans vos mains est également un appareil Bitcoin!

C'est très utile pour les individus qui cherchent à maximiser leur vie privée dans des lieux qui sont hostiles à toute idée de souveraineté financière.

Deuxièmement, le Bowser wallet utilise le code morse pour la saisie. Il s'agit de loin de la fonction la plus "geek" de tous les hardware wallets présentés, et ça signifie concrètement que vous devez soit être en possession d'une feuille détaillant le code Morse, soit l'avoir mémorisé afin d'être capable de taper chaque lettre de cet alphabet.



Là encore, comme la plupart des gens n'ont aucune idée du fonctionnement du Morse (et peuvent même potentiellement le confondre avec le Braille), cette fonction s'avère excellente pour la confidentialité.

Mais l'inconvénient est aussi qu'elle rend concrètement l'appareil plus difficile à utiliser, pour les propriétaires de ce hardware wallet. En fonction du modèle de menace que vous cherchez à mitiger, vous devez donc évaluer dans quelle mesure vous avez besoin de cette complexité supplémentaire.

Le hardware wallet Bowser est un dispositif plutôt cypherpunk puisqu'il associe la confidentialité des jeux vidéo et du Morse à la commodité d'utilisation d'un ordinateur compact à usage général. Vous pouvez vous débarrasser de l'appareil à tout moment et le remplacer par un nouveau – assurez-vous simplement d'avoir votre sauvegarde dans un endroit sûr.

Actuellement, Bowser est conçu pour fonctionner avec le wallet Electrum et utilise la norme PSBT (Partially Signed Bitcoin Transaction) pour signer les transactions.

Cela signifie que ce wallet devrait également être en mesure de fonctionner avec la plupart des wallet du marché.



Pour plus d'informations et afin de mieux comprendre ce qu'est exactement le Bowser wallet, écoutez Ben Arc dans le podcast S8E9 de Bitcoin Takeover.

TREZOR

Putting control in your hands.

Take control of your Bitcoin with a Trezor hardware wallet.
Boost your privacy and manage coins securely, with the integrity and independence of open-source design.



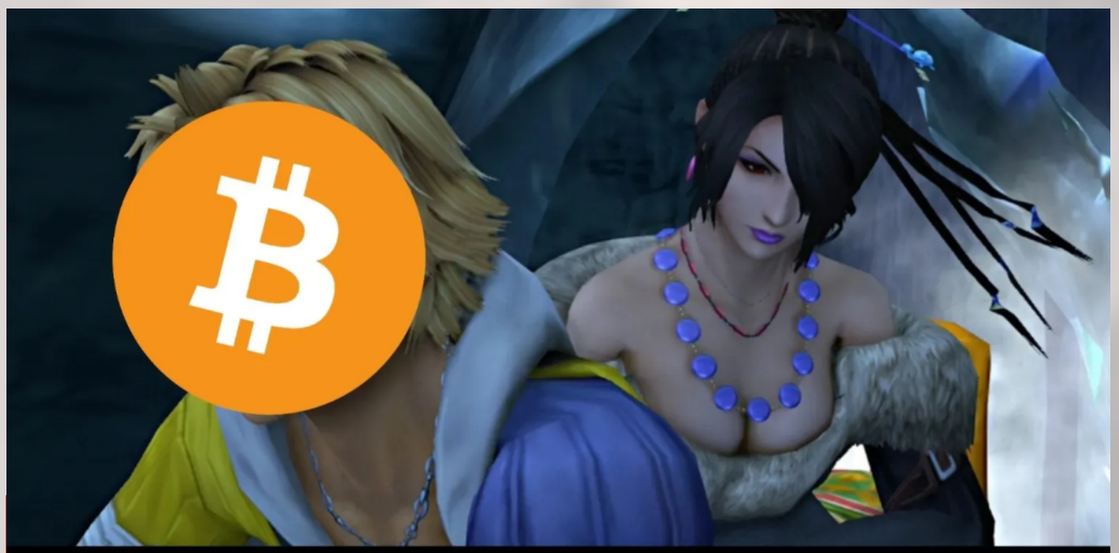
Trezor
Model One

Simple durable design
Monochrome trusted display
PIN and Passphrase
Standard backup

Trezor
Model T

Large comfortable touchscreen
Full-color trusted display
PIN and Passphrase
Standard or Shamir backup

Find out more at **trezor.io**



Pourquoi Les Bitcoiners Devraient Jouer À Final Fantasy X

Après avoir passé près de 80 heures à jouer à la version remasterisée de Final Fantasy X, le RPG d'aventure épique de 2001 de Square Enix, j'en suis arrivé à la conclusion que les personnages principaux ont beaucoup de points communs avec les bitcoiners. J'ai conscience que ça peut paraitre un peu tiré par les cheveux et que ma théorie peut aisément être démontée en objectant que n'importe qui passant trop de temps dans un monde fictif finit par projeter des idées personnelles sur l'action.

Mais je vous promets que Final Fantasy X a vraiment quelque chose de spécial et que les bitcoiners seront sidérés par la fin du troisième acte. En gros il s'agit d'une histoire où se mêlent désillusion et révélation, et dans laquelle cinq adolescents accompagnés de leur mentor plus expérimenté embarquent pour un voyage supposé suivre une tradition séculaire.

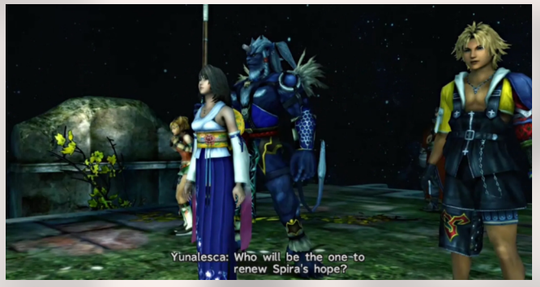
Je ne souhaite pas gâcher le plaisir que procure la découverte des événements qui se dévoilent peu à peu, mais disons simplement qu'en chemin, des nombreux rebondissements inattendus surviennent. C'est certes le cas dans l'ensemble des jeux Final Fantasy, mais dans celui-ci, à un moment donné, les personnages principaux annoncent en substance : "On s'en fout de votre tradition pourrie ! On a trouvé un meilleur moyen et on refuse de perpétuer ce cercle vicieux qui est le votre". Dans mon esprit, ça a résonné comme une évidence et ça faisait écho à l'attitude générale des bitcoiners : notre tendance à défier l'ordre établi et à travailler pour tracer notre propre route avec la volonté constante d'aller de l'avant.

Mais ce n'est pas tout, il existe une autre ressemblance troublante entre Final Fantasy X et Bitcoin : il se dégage une forte impression de responsabilité et d'honneur qui guide les héros et les maintient dans leurs principes idéaliste. Même alors qu'ils



découvrent avoir été au service d'une religion frauduleuse, dont le but n'a jamais été de propager la vérité mais plutôt de contrôler et même encourager l'ignorance, ils persévèrent et continuent par eux même avec leurs propres moyens.

Tidus, Yuna, Wakka, Lulu, Rikku, Kimahri et Auron n'abandonnent pas leur mission au moment où ils découvrent que tout ce qui les entoure n'est qu'un vaste mensonge servant à dissimuler une vérité bien plus laide. Au contraire, ils unissent leurs efforts pour essayer de corriger leur monde et faire en sorte que ce cycle immuable arrête de se répéter.



Ça vous rappelle quelque chose? C'est parce que le rebondissement de la fin du troisième acte (que je ne révélerai pas ici parce que je caresse toujours l'espoir que vous allez jouer à Final Fantasy X) est très similaire au vécu éprouvé par les bitcoiners. On ne veut pas sacrifier notre existence au sein de ce système corrompu; à la place on fait de notre mieux pour construire une meilleure réalité.

On passe la majeure partie de notre vie à faire confiance à un système censé agir dans notre intérêt et considéré comme étant idéal. Et puis un jour, on finit par déceler que le confort et les espoirs dont nous abreuvent nos dirigeants ne sont que des dédommagements reçus en échange de notre docilité. Presque tous les dés sont pipés en notre défaveur mais le système monétaire se révèle être celui le plus insupportable de tous; en effet on passe un tiers de notre vie à travailler (voir même encore plus si on bosse sur des projets personnels) et en contrepartie de notre temps on reçoit une unité monétaire qui se déprécie avec le temps et qui est sans cesse dévaluée par des décisions politiques; cette constatation est vraiment exaspérante.

Et puis on découvre Bitcoin et on se prend de plein fouet un instant "caverne de Platon" – on voit d'un coup la réalité telle qu'elle est et on tente de déterminer la vie qui devrait être la notre fort de ce constat. L'option pessimiste consiste à poser un regard amer sur cette situation et de remplir vaguement ses journées, tout en observant de loin l'aveuglement des autres gens. La manière plus optimiste est de choisir

d'éduquer ceux qui nous entourent avec à l'esprit le désir d'un monde plus juste. Et c'est exactement cette décision que prennent les protagonistes de Final Fantasy X.

Bien sûr, on peut trouver à l'histoire des interprétations religieuses, politiques, financières, voir même sur la parentalité. C'est d'ailleurs peut-être pour ça que le jeu est régulièrement salué comme un chef-d'œuvre de la génération PlayStation 2 et vu comme l'un des meilleurs volets de la série des Final Fantasy. Et même si certaines de ces divulgations peuvent paraitre évidentes, voir banales, un rappel régulier de notre rôle dans ce vaste projet est toujours utile.

J'ai tendance à penser que les bitcoiners ont au fond d'eux des intentions aussi pures que celles des héros de Final Fantasy – ils peuvent certes parfois s'abriter derrière des images d'individus "toxiques" ou inaccessibles, mais au delà de cette façade, ils demeurent des chercheurs et des colporteurs de vérité. Cette antipathie est le plus souvent le fruit de convictions sans failles – chose que n'aura jamais vraiment aucun altcoin, dans la mesure où une vaste majorité de leurs communautés sont uniquement motivés par l'appât du gain et leurs fantasmes de richesses futurs.

Après avoir terminé Final Fantasy X, le mieux que je puisse faire c'est de recommander à tous les bitcoiners d'y jouer. Certes, le jeu a des aspects très répétitifs et un fonctionnement inhérent à la plupart des



J-RPG. Mais l'histoire est carrément géniale et ce jeu contribuera à vous rappeler quel genre de personne vous êtes vraiment et ce que vos connaissances couplées à vos convictions devraient engendrer comme démarche de votre part.

Final Fantasy X est actuellement disponible sur PC (via Steam), PlayStation 4/5, Xbox One, Nintendo Switch, et évidemment sur la PlayStation 2.

Le jeu coûte environ 25€ et il est accompagné de X-2, une suite directe bien plus banale à laquelle je jouerai probablement plus tard pour y déceler des indices d'hyberbitcoinisation. Si vous ne souhaitez pas jouer au jeu et que vous voulez juste regarder les cutscenes qui vous exposent l'histoire, il existe sur Youtube 11 heures de contenu qui sont disponibles gratuitement.

D'un côté, les bitcoiners qui aiment les jeux vidéo devraient clairement jouer à Final Fantasy X; et de l'autre, les gamers qui ont déjà fini Final Fantasy X auront certainement un grand flash lorsqu'ils commenceront à en lire davantage sur Bitcoin, car ça pourrait leur ouvrir les yeux sur le fait qu'une série de désenchantement peut parfois être salutaire et déboucher sur des solutions au monde qui nous entoure.



MAACHI

const char* pszTimestamp =
"The Times 03/Jan/2009 Chancellor
on brink of second bailout
for banks";



Comment je suis presque devenu riche en minant Bitcoin sur SlushPool pendant un mois

Comment Je Suis Presque Devenu Riche En Minant Bitcoin Sur SlushPool Pendant Un Mois

Quand mon ami AdventureDr m'a proposé de faire tourner un Antminer S9 pendant un mois et de me laisser les récompenses si je lui envoyais un magazine BTCTKVR en échange, je n'ai pas pu refuser cette offre si généreuse. Pour me préparer à cet évènement spécial pour moi, j'ai ouvert un compte Slush Pool et j'ai envoyé à AdventureDr les informations nécessaires pour relier le S9 à mon wallet Bitcoin.

Ainsi, pendant les 30 jours qui ont suivi, mon nouvel "employé" a participé à la découverte de 200 blocs Bitcoin. Au cours de cette période, chaque nouveau bloc trouvé offrait une récompense de 6,25 BTC. Ce qui signifie qu'en un mois, l'Antminer S9 a contribué avec succès à ajouter 1250 bitcoins au supply.

Donc je devrais être riche maintenant, non? Bah non… En fait, avoir rejoint Slush Pool signifie que j'ai opté pour un minage collaboratif avec d'autres "travailleurs" du monde entier. Au lieu de tenter d'obtenir la totalité de la récompense pour moi-même avec des chances extrêmement faibles, j'ai opté pour des récompenses de minage bien plus fréquentes mais également bien plus réduites.

Avec un hashrate d'environ 13 terra hash par seconde (soit 13 mille milliards h/s), l'Antminer S9 a été l'un des ~143.000 travailleurs de Slush Pool qui a généré une sortie de 7,272 exa hashes (7272 millions de milliards h/s). Par conséquent, le dispositif qu'AdventureDr a fait tourné pour moi n'a produit que ~0,0000179% de la preuve de travail de l'ensemble de la pool de minage.

Au moment de l'écriture de cet article, le réseau Bitcoin est sécurisé par un hashrate de 161,9 Eh/s. Ça signifie que Slush Pool ne produit que 4,49 % de l'ensemble de la preuve de travail, et que l'Antminer S9, qui m'a été offert, fournit 0,000008 % de la sécurisation de Bitcoin. Ce pourcentage



apparemment insignifiant se reflète également dans les récompenses de minage que j'ai reçues.

Au cours de mon mois en tant que mineur à distance, j'ai gagné un total de 0,00237392 BTC (2373,92 bits, ou 237,392 satoshis), qui avec un cours de 61.258 $ au moment où cette expérience a eu lieu étaient évalués à 145,82 $. Mon Antminer S9 a produit ~0,00019% du revenu de Slush Pool sur les 250 bitcoins pendant ces 30 jours.

Ces Gains De Minage Ne Tiennent Pas Compte Des Coûts D'équipement, D'électricité Et D'entretien.

En moyenne, un Antminer S9 d'occasion coûte environ 600 dollars sur eBay. Et la consommation d'énergie de ce mineur ASIC est de 1800 watts par heure, ce qui représente 1296 kilowatts par mois. A l'endroit où j'habite, un kilowatt coûte environ 15 cents. Donc, faire fonctionner le S9 pendant 30 jours ne me coûterait pas moins de 194 $. Ce qui signifie que, si je devais vendre les BTC minés pour couvrir les coûts électriques, je perdrais 48,18 $ par mois.

Heureusement pour moi, je garde tous les BTC et ma facture d'électricité sera ce mois-ci la même que tous les autres mois précédents- AdventureDr aimait beaucoup le magazine BTCTKVR et a fait fonctionner le mineur ASIC pour moi depuis son installation dédiée. Mais si je devais acheter l'Antminer S9, dans un premier temps je devrais débourser 600 $ environ et ensuite je devrais payer une facture d'électricité mensuelle de 194 $ pour le faire fonctionner.

J'atteindrais certainement le seuil de rentabilité et récupérerais mon investissement initial si je pouvais me permettre de HODL pendant que le prix des BTC augmentera dans les années à venir. Mais d'un point de vue économique, il serait beaucoup plus logique que j'utilise les 600 dollars et le coût énergétique de 194 dollars par mois pour acheter des bitcoins. Dans le même laps de temps, j'obtiendrais un retour sur investissement bien plus important et je n'aurais jamais à gérer les inquiétudes liées à la gestion d'une opération de minage non-rentable.

Naturellement, on pourrait m'opposer deux arguments :

1. que je devrais acheter une machine plus efficace (plus de Th/s avec la même consommation énergétique) qui permettrait de tirer un profit mensuel et finalement d'atteindre le seuil de rentabilité sur investissement ;

2. que je devrais déplacer l'Antminer S9 dans un endroit où le coût de l'électricité rend le minage rentable (comme c'est le cas d'AdventureDr).



Si C'est Plus Rentable D'acheter Des Bitcoins Que De Les Extraire, Pourquoi Se Donner Tant De Mal?

En fait, il y a deux raisons très importantes à ça. Tout d'abord, il est important de contribuer à la sécurité du réseau Bitcoin. On ne devrait pas le laisser se centraliser progressivement dans des grands centres qui ont obtenus les tarifs d'électricité les moins chers et qui tirent parti des économies d'échelle pour réaliser d'énormes bénéfices. Bien sûr, ils sont garant de la robustesse parce que c'est dans leur intérêt financier de maintenir leur opération 7 jours sur 7 et 24 heures sur 24. Mais ils sont en contrepartie également plus faciles à réguler et à démanteler par les gouvernements.

Durant la courte période où Satoshi officiait en tant que développeur, éducateur et conseiller technique, il a fait part de sa vision du minage Bitcoin comme une chose que tous les nœuds étaient en capacité de faire avec leur CPU. La compétition pour découvrir le prochain bloc se devait d'être un processus que tous les participants devaient poursuivre individuellement. Dans le livre blanc, Nakamoto a même défini la preuve de travail comme "en substance un CPU = un vote".

Ce type de décentralisation garantit la résistance à la censure du réseau et réduit les chances d'avoir un acteur puissant qui puisse attaquer ce dernier – au-delà des incitations, il est techniquement et informatiquement bien plus difficile d'avoir une seule unité centrale malveillante dont la puissance de calcul dépasse les efforts additionnés de tous les mineurs honnêtes.

Mais en novembre 2010, Satoshi a observé la montée en puissance de l'approche collaborative de Slush Pool – une découverte qui allait changer à jamais l'économie et la théorie des jeux du minage Bitcoin. Le cypherpunk tchèque Marek "Slush" Palatinus s'est posé la question suivante : "Et si les mineurs, au lieu d'être en concurrence les uns avec les autres pour obtenir la totalité de la récompense de bloc, travaillaient ensemble pour découvrir les blocs plus rapidement et partageaient ensuite les bitcoins nouvellement créés en fonction de leur contribution ?".

Depuis lors, on a assisté à l'essor des pools de minage et on a pu observer les différentes dynamiques mises en jeu dans cet oligopole issu des puissances de hachage. Les mineurs désirant obtenir des récompenses plus fréquentes se sont mis à rechercher alors la pool qui leur accorderait



la plus grande part de la récompense de bloc au taux le plus constant. Au lieu de faire du minage en solo avec des chances équivalentes à celles de gagner à la loterie, ils allaient mettre leur puissance de hachage en commun pour être payés plus souvent et être en mesure de financer leurs opérations de manière plus prévisible.

En théorie, aucune pool ne devrait devenir trop importante et potentiellement menaçante pour l'immuabilité de la blockchain Bitcoin. Mais en pratique, Bitmain a par le passé contrôlé plus de 40 % du taux de hachage en 2018, et à l'époque, les implications de cette question de centralisation du minage ont suscité de vives inquiétudes. Des craintes similaires étaient déjà apparues en 2014, lorsque GHASH.io contrôlait environ 40% du taux de hachage, alors que BTC Guild avait une part d'environ 25% dans le même temps.

Bien sûr, les pools de minage ne sont pas des entreprises qui contrôlent tous les appareils qui travaillent pour elles. De nombreux participants sont des indépendants qui optent simplement pour la pool qui les rémunère le mieux pour leur travail à un instant T. Mais hypothétiquement, si quelques pools dominantes unissent leurs forces en vue de réorganiser les blocs et d'inverser des transactions, ils peuvent y parvenir. Et on devrait tout faire pour éviter ce scénario.

Le minage indépendant à la maison reste essentiel pour le réseau Bitcoin: il contribue à la décentralisation du taux de hachage et augmente la résistance à la censure des transactions. Car oui, les mineurs peuvent choisir de ne pas inclure certaines transactions provenant d'adresses figurant sur une liste noire (avec un coût qui est simplement celui de ne pas percevoir les frais de transaction payés). Par conséquent, le minage altruiste est primordial car il permet de supprimer les discriminations et donc d'augmenter la fongibilité des bitcoins en tant que monnaie. Même si ce minage n'est pas toujours rentable en termes de monnaie fiat, son utilité est essentielle.

Penchons-nous maintenant sur la deuxième raison de miner Bitcoin, qui est plus égoïste et qui a plus à voir avec l'état de la politique et les lois humaines : les BTC nouvellement émis ne sont pas KYC (pas attachés à une identité dans le monde réel). Ça signifie que vous recevez des bitcoins qui ne sont pas "corrompus" par un dépositaire réglementé qui désanonymise les transactions. Le minage est beaucoup plus privée que l'achat auprès d'un exchange, et il y a même des particuliers ou des entreprises qui choisissent d'acheter leurs bitcoins directement auprès des mineurs pour éviter toute forme de traçabilité documentée.

Dans les pays où Bitcoin est interdit ou excessivement surveillé, le minage aide les gens à échapper à Big Brother. Ceux qui vivent sous des régimes totalitaires peuvent avoir besoin de miner des BTC pour gagner une monnaie qui à la faculté de leur permettre d'être libres et souverains. Et dans bien des cas, ils ont besoin de Bitcoin pour soudoyer des fonctionnaires corrompus s'ils veulent être autorisés à commencer une nouvelle vie ailleurs.



Les Arguments En Faveur Du Minage Bitcoin À La Maison

Pour atteindre nos objectifs de décentralisation, on a besoin d'ASICs SHA-256 conçus pour un usage domestique. Il ne s'agit pas de rigs de minage industriels réaffectées, mais d'appareils que tout le monde peut faire fonctionner dans son salon avec à la clé un minimum de bénéfices. Un produit remarquable qui a attiré mon attention est le Futurebit Apollo BTC. Il a un rendement d'environ 3 Th/s pour une consommation électrique de 200 Watts, avec un mode Eco supplémentaire qui lui permet de ne consommer que 125 Watts tout en étant plus silencieux.

J'ai fait un rapide calcul et, si j'utilisais l'Apollo au lieu de l'Antminer, je ferais un bénéfice mensuel de 1 $ (au prix actuel du BTC). Ça signifie qu'il me faudrait environ 800 mois pour récupérer mon investissement de départ, en supposant que le coût de l'électricité, le prix de Bitcoin et la difficulté de minage restent constants (ce qui est clairement impossible)

Mais bon, encore une fois l'intérêt de se procurer un tel appareil n'est pas de s'enrichir, mais de soutenir le réseau. Avec 150 watts/heure, il consomme 10 fois moins d'énergie qu'un climatiseur économique en fonctionnement continu. Et pendant l'hiver, je peux choisir d'utiliser le mode Turbo afin de produire plus de chaleur et garder ma chambre au chaud (ce serait d'ailleurs pas une mauvaise idée de réduire ma dépendance au gaz naturel).



Il ne s'agit en aucun cas d'une pub cachée pour le BTC miner Apollo de Futurebit. Leur appareil est cher pour ce qu'il fait et il est produit en si petites quantités qu'il est toujours épuisé avant que je n'aie la chance d'en acheter un (ça m'est déjà arrivé 3 fois cette année). Je sais que des résultats identiques peuvent être obtenus en downclockant un ASIC "industriel" plus ancien et plus abordable, mais la fiabilité du matériel est toujours discutable.

En fait, j'adorerais que davantage d'entreprises soient idéologiquement positionnées dans cette direction de décentralisation du minage de Bitcoin via les individus. L'idéal serait d'avoir un petit mineur, économe en énergie et silencieux, qu'on pourrait garder à côté de notre routeur Internet. Tout comme on utilise des nœuds Raspberry Pi, on devrait également pouvoir disposer d'un matériel de minage similaire et de pools qui le prennent en charge. En conformité avec l'esprit "don't trust, verify", on devrait diminuer notre dépendance à l'égard des énormes fermes de minage, qui se conforment aux lois et demeurent fragiles politiquement.

Oui, nos noeuds peuvent rejeter les blocs créés par des mineurs malhonnêtes. Mais à l'opposé, les mineurs tout en respectant les règles de consensus du réseau Bitcoin peuvent très bien choisir de ne jamais inclure les transactions que vous diffusez. Il n'y a rien que les nœuds puissent faire pour pousser les mineurs à écrire une certaine transaction dans un bloc Bitcoin. Et cette résistance à la censure ne nous est pas assuré par Satoshi, le livre blanc ou une quelconque croyance idéologique dans les vertus du réseau Bitcoin – nous devons la revendiquer en faisant tourner nos propres opérations avec notre propre matériel.



Au final, je ne me suis pas enrichi en minant Bitcoin. Mais j'ai appris des leçons importantes sur la rentabilité, les économies d'échelle, les limites et l'obsolescence technique des ASICS, et comment les États-nations peuvent nous décourager de miner en ajoutant des taxes supplémentaires sur l'électricité. Mais surtout, j'ai redécouvert l'importance de la décentralisation volontaire. Nous ne devons pas attendre des autres qu'ils sécurisent honnêtement le réseau Bitcoin – ils ont peut-être les fermes, mais de notre côté on a le nombre.

Cours Rapide Et Intensif Sur Le Minage Bitcoin

Le minage Bitcoin est le processus nécessitant une forte intensité énergétique qui sécurise le réseau Bitcoin. Toutes les 10 minutes environ, un nouveau bloc est découvert – et le premier mineur à résoudre un problème mathématique complexe est rémunéré avec la récompense du bloc et les frais de transaction que les utilisateurs ont payés pour donner la priorité à leur transfert.

En échange de la sécurité qu'ils apportent au réseau, les mineurs Bitcoin participent à cette course où le vainqueur rafle l'ensemble de la mise. La production de chaque unité de BTC a un coût énergétique réel, et il est toujours plus coûteux d'attaquer le système que d'y participer honnêtement. Fondamentalement, la sécurité du réseau Bitcoin repose sur l'appât du gain dans un climat de concurrence et un intérêt égoïste des mineurs.

Le système est basé sur la preuve de travail du Dr Adam Back, qui a été intégrée pour la première fois dans hashcash en 1997. Dans sa première itération, le "minage" était un moyen d'empêcher le spam d'e-mails. Pour s'assurer que les expéditeurs ne remplissaient plus les boîtes de réception d'un nombre illimité de destinataires sans aucun coût financier pour eux, les expéditeurs d'e-mails devaient soit utiliser la puissance de traitement de leurs ordinateurs pour extraire du hashcash, soit effectuer un payement pour chaque e-mail. De cette manière, le spamming occasionnait pour eux des coûts financiers ou en puissance de calcul.

Satoshi Nakamoto a repris les principes de hashcash et les a utilisés pour résoudre le problème des généraux byzantins

(également connu sous le nom de Byzantine Fault Tolerance). Essentiellement, la question “comment s’assurer que des participants décentralisés qui ne communiquent pas entre eux se coordonnent pour atteindre le même objectif de manière honnête” a été résolue grâce à la preuve de travail et aux incitations économiques. Ça fait partie de ce qu’on appelle parfois le “consensus de Nakamoto”.

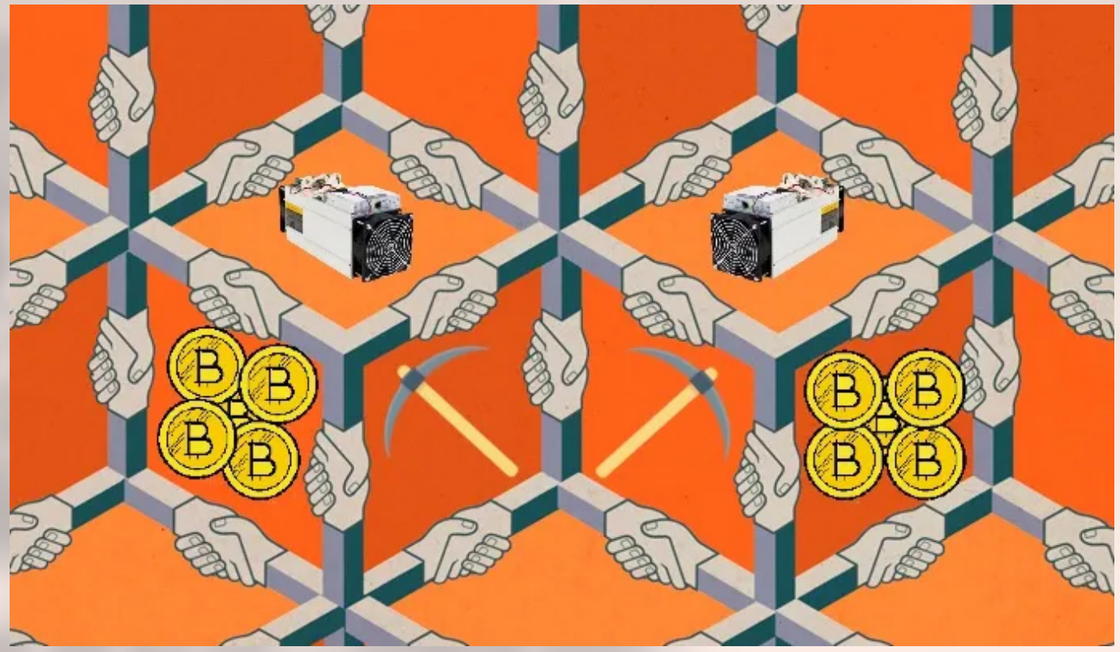
La blockchain Bitcoin est régie par les lois de la physique, et plus précisément par l’entropie, conséquence de la première loi de la thermodynamique. Chaque événement est rendu possible par la consommation d’énergie, et devient donc prouvable et irréversible. Ce point est de la plus haute importance pour la sécurité des transactions, car elles doivent être résistantes à toute politique humaine.

Il est généralement admis qu’après l’extraction de six nouveaux blocs, le coût d’une attaque visant à réorganiser la blockchain est beaucoup trop élevé pour annuler une transaction ancienne. Le mathématicien espagnol Ricardo Perez-Marco et le chercheur français Cyril Grunspan ont même publié un article universitaire dans lequel ils affirment que deux confirmations du réseau sont plus que suffisantes pour déterminer le caractère définitif d’une transaction, notamment en raison des coûts de plusieurs millions de dollars qu’impliquerait une attaque contre celle-ci.

Les mineurs Bitcoin sont en concurrence pour une récompense de bloc qui diminue de 50 % tous les 210 000 blocs (environ 4 ans). Au début, la récompense était de 50 bitcoins par bloc. En novembre 2012, le 210.000ème bloc Bitcoin a été miné et la nouvelle récompense est descendue à 25 BTC. A partir du bloc 420.000 (juillet 2016) jusqu’au bloc 630.000 (mai 2020), la résolution du problème mathématique complexe tout en sécurisant le réseau a été récompensée par 12,5 BTC. Et à l’heure actuelle, la récompense de bloc est de 6,25 BTC, puis elle sera à nouveau divisée par deux après le bloc 840.000 (en 2024).

C’est comme ça que la totalité de l’offre des 21 millions de bitcoins sera émise. Il faudra attendre l’année 2140 (la 34e époque de division par deux) pour que l’ensemble des unités soient en circulation. Mais ça ne signifie pas pour autant que le minage va s’arrêter. La conception pensée par Satoshi Nakamoto permet d’offrir une seconde incitation économique au minage, à savoir les frais de transaction. Dans quelques décennies, la somme de ces frais sera supérieure à la récompense de découverte de bloc.





Chaque transaction ce sont des données qui occupent de l’espace dans les blocs Bitcoin. Ainsi, pour que votre transaction soit incluse dans un bloc, vous devez payer un certain nombre d’unités BTC pour chaque octet de données que vous allez occuper. Lorsque la demande augmente, un jeu de priorités se met en place en faveur du plus offrant – les utilisateurs Bitcoin qui paient le plus pour leur transaction sont ceux qui recevront leurs confirmations en priorité.

Ainsi, l’argent payé en frais de transaction va au mineur (ou au pool de minage) qui trouve le bloc. Ça signifie que la récompense totale du bloc pour le mineur est constituée de la récompense déterminée pendant l’époque correspondante (qui est constante sur 210 000 blocs), plus les frais de transaction.

Par exemple, en 2021, pour le bloc 706468, les mineurs ont perçu 6,25 BTC comme récompense de bloc, ainsi que ~0,05 BTC supplémentaires provenant des frais de transaction (à un tarif médian de 4 sat/octet).

Mais alors plus le nombre de mineurs augmente, plus la difficulté pour découvrir un bloc va également augmenter de façon exponentielle, non? Ça signifie que toujours plus d’énergie devra être consommée pour produire des bitcoins au fil du temps? Alors, pas tout à fait. Satoshi Nakamoto a inclus dans sa conception un système de réajustement régulier de la difficulté de minage.

En effet, après chaque période de 2016 blocs, la difficulté est réajustée en fonction de l’activité existante: si davantage de puissance de hachage a été ajoutée au cours du cycle précédent de 2016 blocs, alors la difficulté sera augmentée.

Mais si dans le cas contraire des mineurs ont cessé leur activité en raison d’intérêt économique qui leur sont propres (le coût de l’électricité est devenu plus élevé que la récompense par exemple), alors la difficulté de recherche des blocs va diminuer.

Ce processus dynamique engendre des opportunités afin de saisir le moment idéal auquel démarrer le minage, et conduit également à une recherche permanente des coûts électriques les plus bas. Lorsqu’un mineur cesse son activité et que par conséquent la difficulté diminue, il y aura toujours quelqu’un d’autre à l’autre bout de la planète pour profiter de cette chance d’obtenir plus de bitcoins avec moins d’effort.

Comment Je Suis Presque Devenu Riche En Minant Bitcoin Sur SlushPool Pendant Un Mois



Et il se trouve que le type d'énergie le plus abordable est celui qui est généré à partir de sources renouvelables. Le minage Bitcoin par preuve de travail a enclenché une quête mondiale d'électricité bon marché : en Chine, les mineurs ont utilisé des roues à eau (énergie hydroélectrique) ; aux États-Unis, des mineurs brûlent le gaz naturel qui est normalement gaspillé lors de l'extraction du pétrole ; au Salvador, c'est l'énergie géothermique des volcans qui est utilisée pour alimenter les mineurs ASIC…

Partout sur la planète, le surplus d'énergie que les centrales électriques produisent et que les réseaux ne peuvent pas transporter jusqu'aux consommateurs peut être utilisé pour sécuriser le réseau Bitcoin et générer des profits supplémentaires. Ce que certains décrivent comme un processus de gaspillage encourage en fait l'expansion et le développement des énergies renouvelables.

Le minage Bitcoin est l'une des industries les plus dynamiques au monde. Depuis janvier 2009, on a réussi à passer du concept initial "un CPU, un vote" au minage par GPU, à toute une industrie qui a donné naissance à un commerce lucratif de machines ASIC (Application-Specific Integrated Circuits, ou ordinateurs spécialisés qui ne peuvent effectuer qu'une seule tâche de manière très efficace).

Le minage à domicile a rapidement laissé la place aux fermes industrielles, et pendant un certain temps, la majorité de cette activité avait lieu en Chine.

Mais depuis le second semestre 2021, en raison de certaines politiques autoritaires dans ce pays, les nouveaux leader du minage de Bitcoin sont désormais officiellement les États-Unis.

Cependant, je garde espoir que des sociétés de matériel informatique vont un jour trouver des moyens créatifs qui permettront de ramener le minage Bitcoin dans les foyers des particuliers.

Aux 4 coins du monde, des personnes ingénieuses ont déjà trouvé le moyen d'utiliser la chaleur générée par les mineurs Bitcoins pour chauffer leur maison ou faire bouillir de l'eau pour leur douche.

En fin de compte, l'ingéniosité humaine est infinie et nous allons assister à de nombreux développements si brillants que nos esprits ne peuvent même pas les concevoir pour l'instant.

Et tant que ça rend le réseau Bitcoin plus décentralisé et l'aide à atteindre son objectif de séparer l'argent de la politique humaine, je vote complètement pour.





LE LONG CHEMIN QUI A MENÉ À TAPROOT

Le Long Chemin Qui A Mené À Taproot

Taproot est le changement le plus important qui a été apportée au code de Bitcoin ces dernières années. Il a suivit la même méthode d'activation par soft fork qui avait été utilisée pour SegWit en 2017, à la différence près que cette fois-ci, le test (trial) a consisté à sécuriser 90% des blocs minés durant la période de 2016 blocs qui constitue une époque (environ 2 semaines).

D'un point de vue technique, Taproot reprend la crême de trois propositions d'amélioration majeures : les signatures de Schnorr (décrites dans le BIP 340), les branches de Merkle (également appelées MAST ou Merklelized Abstract Syntax Tree, décrites dans le BIP 114 et le BIP 117), ainsi que de nouveaux opcodes (Taproot, Grafroot, G'root et cross-input aggregation).

Comme l'expliquent les développeurs de Bitcoin Core Pieter Wuille, Jonas Nick et Anthony Towns dans leur proposition finale de Taproot BIP 341, leur travail ne consiste pas en une encapsulation de toutes les idées précédemment citées – car l'ajout d'un trop grand nombre de modifications du code impliquerait un processus de revue plus compliqué et une augmentation du risque d'ajouter des bugs indésirables. Dans le même temps, il ne s'agit pas non plus d'une tentative de pousser séparément ces propositions – une trop grade quantité d'upgrades épuiseraient les opérateurs indépendants de nœuds, tout en réduisant les avantages de cette approche sélective. Les auteurs du BIP ont choisi de le présenter comme un "compromis établissant un équilibre", mais je préfère personnellement le voir comme un affinement qui a privilégié les meilleures fonctionnalités à disposition pour déboucher sur un efficacité optimale.

Taproot, c'est un peu comme la combinaison de trois plats pour lesquels on aurait réduit les portions, mais en conservant tout de même leur goût et leur valeur nutritionnelle pour chacun d'eux. On peut dire qu'il s'agit d'une autre avancée significative dans le processus visant à rendre Bitcoin plus efficace; au lieu d'une mise à l'échelle via de plus gros blocs comme le font de nombreux altcoins existants, le réseau cherche sans cesse à optimiser l'efficacité et la confidentialité des petits blocs existants pour que cela puisse bénéficier à l'ensemble des utilisateurs.

Dans un article précédent, j'avais fait l'éloge du mécanisme d'activation utilisé et soutenu que le chemin qui a conduit à cet upgrade reflète exactement le type de décentralisation dont Bitcoin a besoin pour réussir en tant que projet. Ici, je vais utiliser le court thread de Pieter Wuille pour tenter de raconter l'histoire de l'activation de Taproot et expliquer ce qui est supposé en découler.

Taproot – Depuis Une Discussion Au Restaurant En 2018 Jusqu'au Lock-In De Juin 2021

Lorsque le bloc 687284 a été miné par F2Pool le 12 juin 2021, le soft fork Taproot avait été signalé par plus de 90% des mineurs qui avaient découvert des blocs durant cette époque. Ça signifiait concrètement que Taproot allait donc finalement pouvoir être activé au bloc de hauteur 709632, événement qui a eu lieu ensuite le 14 novembre 2021 (et ce premier bloc Taproot a lui aussi été miné par F2Pool d'ailleurs).

Cependant, le phénomène Taproot n'est pas apparu du jour au lendemain. L'idée de remplacer l'ECDSA (Elliptic Curve Digital Signature Algorithm) de Bitcoin par les signatures Schnorr est débattue depuis des années au sein de la communauté. Satoshi Nakamoto avait choisi l'ECDSA, moins efficace, car un brevet l'empêchait encore d'utiliser Schnorr jusqu'en 2008, et la norme open source, plus populaire à l'époque, disposait de toute façon de plus de librairies. Ainsi, même si sa conception n'était pas exactement idéale, elle était clairement la plus pratique et la plus raisonnable à ce moment là.

Et pourtant, les bitcoiners rêvaient d'ajouter les signatures Schnorr depuis des années déjà. Une proposition a été formalisée par Greg Maxwell en janvier 2018, quelques mois seulement après que SegWit ait été activé avec succès via UASF (User-Activated Soft Fork). À peu près au même moment, ce même Maxwell a rencontré ses collègues développeurs et cryptographes Pieter Wuille et Andrew Poelstra lors d'un diner à Los Altos, en Californie. Comme l'a décrit Wuille, ses pairs avaient eu une "idée vraiment cool pour cacher les racines Merkle dans des sorties de type P2PK" alors qu'il



avait brièvement quitté la table.

Mais sur Bitcoin, le processus nécessaire entre une séance de brainstorming réussie et la présentation d'une proposition examinée en profondeur peut facilement dépasser 3 ans ou plus. Wuille a donc formalisé la première proposition Taproot en mai 2019 – il ne s'agissait alors que d'un court message à la mailing list des développeurs Bitcoin, mais le texte décrivait déjà les principales caractéristiques du soft fork. Les contributeurs à cette proposition incluaient Jonas Nick, Anthony Towns et Tim Ruffing – qui sont tous restés dans les parages pendant tout le cycle de développement.

Après quelques essais et des observations minutieuses, une version épurée de Taproot a été dévoilée par Wuille en octobre 2019. Cette fois, Wuille et ses collaborateurs ont amputé plusieurs éléments susceptibles de causer des complications inutiles et de potentiellement faire obstacle à l'efficacité recherchée (le plus célèbre étant l'abandon d'un octet de la conception initiale de la clé publique de 32 octets, car il "ne contribuait manifestement pas à la sécurité"). De même, ils ont quadruplé la profondeur des arbres de

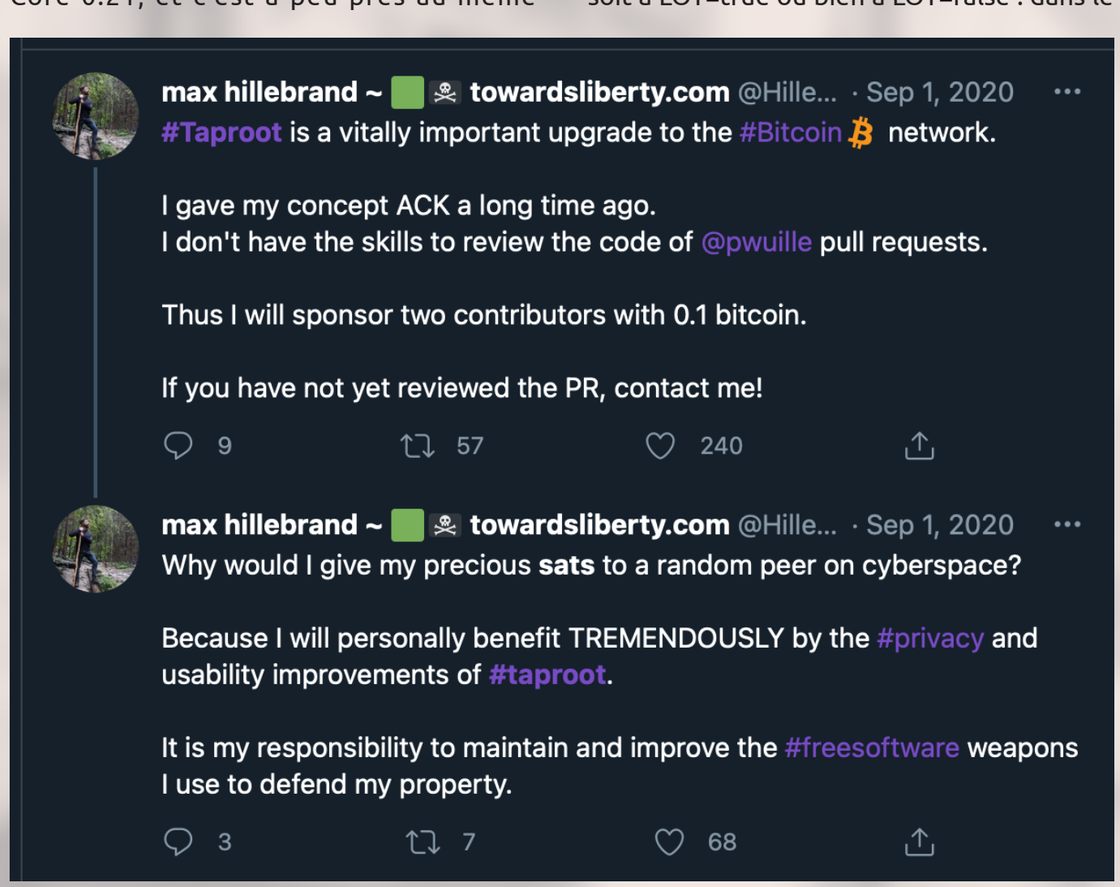
Merkle dans le but d'optimiser le code. Le graal du développement de Bitcoin c'est l'efficacité, et cette deuxième version collait parfaitement avec cet objectif.

Taproot a enregistré ses dernières modifications en août 2020, lorsque le tiebreaker des résidus quadratiques a été supprimé. Ici aussi, il s'agissait encore et toujours d'améliorer l'efficacité. Et lorsqu'une fonctionnalité n'apporte pas les avantages escomptés et entraîne une complexité supplémentaire, elle est tout bonnement supprimée. Ça fait partie de l'éthique du développement de Bitcoin: chaque ligne de code doit compter. Il ne s'agit pas seulement d'une forme de minimalisme, mais surtout d'une recherche constante de l'efficacité maximale.

En octobre 2020, une version finale de Taproot était enfin disponible pour les tests. Les développeurs l'ont merge dans une version préliminaire sur le testnet de Bitcoin Core 0.21, et c'est à peu près au même moment que les débats sur son activation ont commencé à être sérieusement abordés.

Entre-temps, tout au long du processus de développement, des auditeurs indépendants allaient jeter un coup d'œil au code open source. Après tout, c'était l'avenir de la monnaie qui était en jeu et personne n'aurait voulu laisser passer une erreur fatale qui aurait porté atteinte au bon fonctionnement d'un système comme celui de Bitcoin. Des bitcoiners comme Max Hillebrand ont donc offert des bounties (primes) à des experts afin qu'ils examinent en détail chaque ligne du code et s'assurent que rien de litigieux ou de non-optimal n'ait été inclus. Ça fait partie du charme offert par un système décentralisé et au code open source, où tout est visible et pour lequel n'importe qui dans le monde peut contribuer.

Pour ceux qui ont un peu de mémoire, la pierre d'achoppement qui a émergé à ce moment là consistait à montrer son soutien soit à LOT=true ou bien à LOT=false : dans le



[bitcoin-dev] Taproot activation proposal "Speedy Trial"

David A. Harding dave at dtrt.org
Sat Mar 6 03:43:43 UTC 2021

- Previous message: [bitcoin-dev] Supermajority then simple majority Taproot Activation
- Next message: [bitcoin-dev] Taproot activation proposal "Speedy Trial"
- **Messages sorted by:** [date] [thread] [subject] [author]

```
On the ##taproot-activation IRC channel, Russell O'Connor recently
proposed a modification of the "Let's see what happens" activation
proposal.[1] The idea received significant discussion and seemed
acceptable to several people who could not previously agree on a
proposal (although this doesn't necessarily make it their first
choice).  The following is my attempt at a description.

1. Start soon: shortly after the release of software containing this
   proposed activation logic, nodes will begin counting blocks towards
   the 90% threshold required to lock in taproot.[2]

2. Stop soon: if the lockin threshold isn't reached within approximately
   three months, the activation attempt fails.  There is no mandatory
   activation and everyone is encouraged to try again using different
   activation parameters.

2. Delayed activation: in the happy occasion where the lockin threshold
   is reached, taproot is guaranteed to eventually activate---but not
   until approximately six months after signal tracking started.
```

premier cas, les nœuds souverains pouvaient intervenir et rejeter les blocs des mineurs qui ne signalaient pas l'activation de Taproot à la fin de la période d'essai ; et dans le second cas, il n'y aurait aucune conséquence si les mineurs refusaient de se mettre à jour vers Taproot (leur donnant ainsi un droit de veto). Dans tous les cas, la période de signalement aurait duré une année entière.

Ce qui est important c'est que les utilisateurs avaient toujours en tête ce qu'il s'était passé en 2017 avec SegWit. À l'époque, les mineurs avaient refusé de signaler l'activation du softfork dans le temps d'essai imparti. Par conséquent, les nœuds souverains avaient pris sur eux même d'adopter la correction de la malléabilité des transactions – ce qui avait conduit au succès du mouvement UASF (User Activated Soft Fork).

Mais au milieu de ces débats houleux, David Harding avait présenté une proposition de "speedy trial" qui ne durerait que 3 mois et nécessiterait une supermajorité de 90% des blocs minés au cours d'une époque. Ça paraissait être la manière idéale de procéder, puisque tout le monde semblait d'accord pour dire que le code Taproot était prêt et que l'activation n'était qu'une affaire de consentement à mettre à jour le client Bitcoin Core.

Le speedy trial a toutefois connu des débuts difficiles, avec seulement une poignée de pools de minage (dont Slush Pool et Foundry USA) qui signalèrent l'activation de Taproot. Mais les bitcoiners comme à leur habitude n'ont rien lâché et ont continué à faire pression sur les mineurs pour leur demander de signaler leur soutien. Les utilisateurs de Twitter ont fait corps et ont affiché leur soutien à Taproot en utilisant l'émoji bloc vert à côté de leur nom. Toutefois à l'issue la première époque, la situation ne semblait pas bien engagée. Bien que F2Pool ait été le premier grand acteur à avoir rejoint le camp de l'activation, c'était toujours loin d'être suffisant.

La deuxième époque du trial n'a pas été concluante non plus, mais elle était toute proche cette fois. Durant cette période, des pools de minage tels que Poolin, Antpool, BTC.com et Binance Pool ont été poussés à rejoindre le camp de la signalisation. Au cours des derniers blocs de cette époque, c'est devenu évident que la troisième fois serait la bonne. À moins que les mineurs ne décident de revenir sur leur décision de soutenir Taproot, l'activation allait être verrouillée de



manière imminente. Et c'est exactement ce qui s'est passé le 12 juin 2021.

Et Ensuite ?

L'activation de Taproot allait donc pouvoir avoir lieu en novembre 2021, au bloc 709632. Mais d'ici là, il y avait encore beaucoup de pain sur la planche. Du côté des développeurs, les wallets allaient devoir être mis à jour et standardisés. Pour tirer parti des avancées en matière de confidentialité des multisigs, le format MuSig2 allait devoir établir une norme que tous les wallet allaient pouvoir utiliser. De même, les extensions PSBT allaient devoir être améliorées afin de communiquer avec les clés, les scripts et les signatures.

Du côté des utilisateurs, ils allaient devoir mettre à jour les clients de leurs nœuds pour une version supportant Taproot – la plus récente étant la 0.21.1. Il s'agissait et il s'agit toujours de l'étape la plus importante, car tous les efforts de codage et d'activation sont vains s'ils ne sont pas utilisés à leur plein potentiel. Évidemment, tout est facultatif et repose sur l'intérêt des opérateurs de noeuds souverains. Mais il y a des avantages indiscutables à cet upgrade, tant au niveau individuel qu'au niveau du réseau.

J'ai entendu parler de Taproot pour la première fois en 2019, dans un article d'Aaron van Wirdum. Il aura fallu environ deux ans pour que le code soit affiné puis examiné par la communauté, et une demi-année de plus avant que le speedy trial ne réussisse à verrouiller le soft fork avant son activation en novembre par la suite. Ça peut sembler long, mais c'est ainsi qu'il est normal de progresser dans un écosystème décentralisé et véritablement délibératif. Tout doit être optimisé dans les moindres détails, et indubitablement la performance doit primer sur la vitesse d'activation ou la pression exercée par certains acteurs du marché au cours des différentes phases.

Bitcoin est l'exemple parfait d'un système décentralisé qui prend en compte les opinions de tous les utilisateurs et donne à chacun suffisamment de temps pour exprimer ses préoccupations et ses critiques. Et il demeure peu probable que cela ne change à l'avenir : les mineurs et les opérateurs de nœuds exigeront toujours les niveaux de rigueur les plus strictes avant d'exécuter une nouvelle version du client, tandis que les développeurs saisiront chaque opportunité qui se présente à eux pour se démarquer via des ajouts constructifs ou bien des critiques précieuses.

Il reste encore et toujours des améliorations à apporter à la couche de base de Bitcoin et les propositions ne manquent pas, allant des Drivechains à OP_CheckTemplateVerify. Les développeurs travaillent dur afin de faire ce pour quoi ils excellent : tirer le meilleur parti possible de Bitcoin et repousser ses limites de manière créative et efficace.



yITé
TECHNOLOGIES

WE ARE BITCOIN DEVELOPERS

Yité Technologies a pour raison d'être de mettre en place des solutions pratiques et intuitives, tournées vers l'accessibilité aux possibilités qu'offre le protocole Bitcoin.

Nous sommes l'une des premières entreprises spécialisée dans le conseil et le développement de solutions basées sur Bitcoin, du Sénégal et d'Afrique de l'Ouest francophone.

https://yite.tech

+221 77 492 47 30

hello@yite.tech

BTCTKVR



Vaultoro

WASABI WALLET

TREZOR

BRAIINS

LNbits

SATOSHILABS

MAACHI

L'AFRIQUE PARLE BITCOIN

Bitcoin LYON