Sécurité de Bitcoin

2022-03-12

# Sécurité de Bitcoin

Sécuriser le bitcoin est un défi car le bitcoin n'est pas une référence abstraite à la valeur, comme le solde d'un compte bancaire. Bitcoin ressemble beaucoup à de l'argent numérique ou à de l'or. Vous avez probablement entendu l'expression, "La possession est les neuf dixièmes de la loi." Eh bien, en bitcoin, la possession correspond aux dix dixièmes de la loi. La possession des clés pour déverrouiller le bitcoin équivaut à la possession d'espèces ou d'un morceau de métal précieux. Vous pouvez le perdre, l'égarer, le faire voler ou donner accidentellement le mauvais montant à quelqu'un. Dans chacun de ces cas, l'usager n'a aucun recours, comme s'il déposait de l'argent sur un trottoir public.

Cependant, le bitcoin a des capacités que l'argent, l'or et les comptes bancaires n'ont pas. Un portefeuille bitcoin, contenant vos clés, peut être sauvegardé comme n'importe quel fichier. Il peut être stocké en plusieurs exemplaires, même imprimé sur papier pour une copie papier. Vous ne pouvez pas "sauvegarder" de l'argent, de l'or ou des comptes bancaires. Le bitcoin est suffisamment différent de tout ce qui a précédé pour que nous devions également penser à la sécurité du bitcoin d'une manière nouvelle.

## Principes de sécurité

Le principe fondamental du bitcoin est la décentralisation et il a des implications importantes pour la sécurité. Un modèle centralisé, tel qu'une banque traditionnelle ou un réseau de paiement, dépend du contrôle d'accès et de la vérification pour garder les mauvais acteurs hors du système. En comparaison, un système décentralisé comme Bitcoin pousse la responsabilité et le contrôle aux utilisateurs. Étant donné que la sécurité du réseau est basée sur la preuve de travail et non sur le contrôle d'accès, le réseau peut être ouvert et aucun cryptage n'est requis pour le trafic bitcoin.

Sur un réseau de paiement traditionnel, tel qu'un système de carte de crédit, le paiement est ouvert car il contient l'identifiant privé de l'utilisateur (le numéro de carte de crédit). Après le débit initial, toute personne ayant accès à l'identifiant peut "extraire" des fonds et facturer le propriétaire encore et encore. Ainsi, le réseau de paiement doit être sécurisé de bout en bout avec un cryptage et doit garantir qu'aucun espion ou intermédiaire ne puisse compromettre le trafic de paiement, en transit ou lorsqu'il est stocké (au repos). Si un acteur malveillant accède au système, il peut compromettre les transactions en cours *et* les jetons de paiement qui peuvent être utilisés pour créer de nouvelles transactions. Pire encore, lorsque les données des clients sont compromises, les clients sont exposés au vol d'identité et doivent prendre des mesures pour empêcher l'utilisation frauduleuse des comptes compromis.

Bitcoin est radicalement différent. Une transaction bitcoin n'autorise qu'une valeur spécifique à un destinataire spécifique et ne peut être falsifiée ou modifiée. Il ne révèle aucune information privée, telle que l'identité des parties, et ne peut être utilisé pour autoriser des paiements supplémentaires. Par conséquent, un réseau de paiement bitcoin n'a pas besoin d'être crypté ou protégé contre les écoutes clandestines. En fait, vous pouvez diffuser des transactions en bitcoins sur un canal public ouvert, tel qu'un WiFi ou un Bluetooth non sécurisé, sans perte de sécurité.

Le modèle de sécurité décentralisé de Bitcoin donne beaucoup de pouvoir aux utilisateurs. Ce pouvoir s'accompagne de la responsabilité de maintenir le secret des clés. Pour la plupart des utilisateurs, ce n'est pas facile à faire, en particulier sur les appareils informatiques à usage général tels que les smartphones ou les ordinateurs portables connectés à Internet. Bien que le modèle décentralisé de Bitcoin empêche le type de compromis de masse observé avec les cartes de crédit, de nombreux utilisateurs ne sont pas en mesure de sécuriser correctement leurs clés et se font pirater, un par un.

### Développer des systèmes Bitcoin en toute sécurité

Le principe le plus important pour les développeurs de bitcoins est la décentralisation. La plupart des développeurs connaissent les modèles de sécurité centralisés et pourraient être tentés d'appliquer ces modèles à leurs applications bitcoin, avec des résultats désastreux.

La sécurité de Bitcoin repose sur un contrôle décentralisé des clés et sur une validation indépendante des transactions par les mineurs. Si vous souhaitez tirer parti de la sécurité du bitcoin, vous devez vous assurer que vous restez dans le modèle de sécurité du bitcoin. En termes simples : ne retirez pas le contrôle des clés aux utilisateurs et ne retirez pas les transactions de la chaîne de blocs.

Par exemple, de nombreux premiers échanges de bitcoins ont concentré tous les fonds des utilisateurs dans un seul portefeuille "chaud" avec des clés stockées sur un seul serveur. Une telle conception supprime le contrôle des utilisateurs et centralise le contrôle des clés dans un système unique. De nombreux systèmes de ce type ont été piratés, avec des conséquences désastreuses pour leurs clients.

Une autre erreur courante consiste à retirer les transactions "hors chaîne de blocs" dans un effort malavisé pour réduire les frais de transaction ou accélérer le traitement des transactions. Un système "hors chaîne de blocs" enregistrera les transactions sur un registre interne centralisé et ne les synchronisera qu'occasionnellement avec la chaîne de blocs Bitcoin. Cette pratique, encore une fois, remplace la sécurité du bitcoin décentralisée par une approche propriétaire et centralisée. Lorsque les transactions sont hors chaîne de blocs, des registres centralisés mal sécurisés peuvent être falsifiés, détournant des fonds et épuisant les réserves, sans que l'on s'en aperçoive.

À moins que vous ne soyez prêt à investir massivement dans la sécurité opérationnelle, plusieurs couches de contrôle d'accès et des audits (comme le font les banques traditionnelles), vous devez réfléchir très attentivement avant de retirer des fonds du contexte de sécurité décentralisé de Bitcoin. Même si vous disposez des fonds et de la discipline nécessaires pour mettre en œuvre un modèle de sécurité robuste, une telle conception ne fait que reproduire le modèle fragile des réseaux financiers traditionnels, en proie au vol d'identité, à la corruption et au détournement de fonds. Pour tirer parti du modèle de sécurité décentralisé unique de Bitcoin, vous devez éviter la tentation d'architectures centralisées qui pourraient vous sembler familières mais qui finissent par renverser la sécurité de Bitcoin.

### La racine de la confiance

L'architecture de sécurité traditionnelle est basée sur un concept appelé *racine de confiance*, qui est un noyau de confiance utilisé comme base pour la sécurité de l'ensemble du système ou de l'application. L'architecture de sécurité est développée autour de la racine de la confiance sous la forme d'une série de cercles concentriques, comme des couches dans un oignon, étendant la confiance vers l'extérieur depuis le centre. Chaque couche s'appuie sur la couche interne la plus fiable à l'aide de contrôles d'accès, de signatures numériques, de cryptage et d'autres primitives de sécurité. À mesure que les systèmes logiciels deviennent plus complexes, ils sont plus susceptibles de contenir des bogues, ce qui les rend vulnérables aux compromis de sécurité. Par conséquent, plus un système logiciel devient complexe, plus il est difficile à sécuriser. Le concept de racine de confiance garantit que la plus grande partie de la confiance est placée dans la partie la moins complexe du système, et donc la moins vulnérable, tandis que des logiciels plus complexes sont superposés autour d'elle. Cette architecture de sécurité est répétée à différentes échelles, établissant d'abord une racine de confiance dans le matériel d'un système unique, puis étendant cette racine de confiance à travers le système d'exploitation jusqu'aux services système de niveau supérieur, et enfin sur de nombreux serveurs superposés en cercles concentriques de diminution de la confiance.

L'architecture de sécurité Bitcoin est différente. En bitcoin, le système de consensus crée un grand livre public de confiance qui est complètement décentralisé. Une chaîne de blocs correctement validée utilise le bloc de gen’se comme racine de confiance, construisant une chaîne de confiance jusqu'au bloc actuel. Les systèmes Bitcoin peuvent et doivent utiliser la chaîne de blocs comme racine de confiance. Lors de la conception d'une application bitcoin complexe composée de services sur de nombreux systèmes différents, vous devez examiner attentivement l'architecture de sécurité afin de déterminer où la confiance est placée. En fin de compte, la seule chose à laquelle il faut explicitement faire confiance est une chaîne de blocs entièrement validée. Si votre application accorde explicitement ou implicitement sa confiance à autre chose qu'à la chaîne de blocs, cela devrait être une source de préoccupation car elle introduit une vulnérabilité. Une bonne méthode pour évaluer l'architecture de sécurité de votre application consiste à considérer chaque composant individuel et à évaluer un scénario hypothétique où ce composant est complètement compromis et sous le contrôle d'un acteur malveillant. Prenez tour à tour chaque composant de votre application et évaluez les impacts sur la sécurité globale si ce composant est compromis. Si votre application n'est plus sécurisée lorsque des composants sont compromis, cela montre que vous avez mal placé la confiance dans ces composants. Une application bitcoin sans vulnérabilités ne devrait être vulnérable qu'à une compromission du mécanisme de consensus bitcoin, ce qui signifie que sa racine de confiance est basée sur la partie la plus solide de l'architecture de sécurité bitcoin.

Les nombreux exemples d'échanges de bitcoins piratés servent à souligner ce point, car leur architecture et leur conception de sécurité échouent même sous l'examen le plus occasionnel. Ces implémentations centralisées avaient explicitement investi la confiance dans de nombreux composants en dehors de la chaîne de blocs Bitcoin, tels que les portefeuilles actifs, les bases de données de grand livre centralisées, les clés de chiffrement vulnérables et les schémas similaires.

## Meilleures pratiques de sécurité des utilisateurs

Les humains ont utilisé des contrôles de sécurité physique depuis des milliers d'années. En comparaison, notre expérience en matière de sécurité numérique a moins de 50 ans. Les systèmes d'exploitation modernes à usage général ne sont pas très sécurisés et ne sont pas particulièrement adaptés au stockage de l'argent numérique. Nos ordinateurs sont constamment exposés à des menaces externes via des connexions Internet permanentes. Ils exécutent des milliers de composants logiciels de centaines d'auteurs, souvent avec un accès illimité aux fichiers de l'utilisateur. Un seul logiciel malveillant, parmi les milliers installés sur votre ordinateur, peut compromettre votre clavier et vos fichiers, en volant tout bitcoin stocké dans les applications de portefeuille. Le niveau de maintenance informatique requis pour maintenir un ordinateur exempt de virus et de chevaux de Troie dépasse le niveau de compétence de tous, sauf d'une infime minorité d'utilisateurs d'ordinateurs.

Malgré des décennies de recherche et d'avancées en matière de sécurité de l'information, les actifs numériques sont toujours terriblement vulnérables face à un adversaire déterminé. Même les systèmes les plus protégés et les plus restreints, dans les sociétés de services financiers, les agences de renseignement et les sous-traitants de la défense, sont fréquemment piratés. Bitcoin crée des actifs numériques qui ont une valeur intrinsèque et peuvent être volés et détournés vers de nouveaux propriétaires instantanément et irrévocablement. Cela crée une incitation massive pour les pirates. Jusqu'à présent, les pirates devaient convertir des informations d'identité ou des jetons de compte, tels que des cartes de crédit et des comptes bancaires, en valeur après les avoir compromis. Malgré la difficulté de clôturer et de blanchir les informations financières, nous avons vu des vols sans cesse croissants. Bitcoin intensifie ce problème car il n'a pas besoin d'être clôturé ou blanchi; c'est la valeur intrinsèque d'un actif numérique.

Heureusement, le bitcoin crée également les incitations à améliorer la sécurité informatique. Alors qu'auparavant le risque de compromission informatique était vague et indirect, le bitcoin rend ces risques clairs et évidents. La détention de bitcoins sur un ordinateur sert à concentrer l'esprit de l'utilisateur sur la nécessité d'améliorer la sécurité informatique. En conséquence directe de la prolifération et de l'adoption accrue du bitcoin et d'autres monnaies numériques, nous avons assisté à une escalade des techniques de piratage et des solutions de sécurité. En termes simples, les pirates ont désormais une cible très juteuse et les utilisateurs ont une incitation claire à se défendre.

Au cours des trois dernières années, en conséquence directe de l'adoption du bitcoin, nous avons assisté à d'énormes innovations dans le domaine de la sécurité de l'information sous la forme de cryptage matériel, de stockage de clés et de portefeuilles matériels, de technologie multisignature et de séquestre numérique. Dans les sections suivantes, nous examinerons diverses meilleures pratiques pour la sécurité pratique des utilisateurs.

### Stockage Bitcoin physique

Parce que la plupart des utilisateurs sont beaucoup plus à l'aise avec la sécurité physique qu'avec la sécurité des informations, une méthode très efficace pour protéger les bitcoins consiste à les convertir sous forme physique. Les clés Bitcoin ne sont rien de plus que de longs chiffres. Cela signifie qu'ils peuvent être stockés sous une forme physique, telle qu'imprimés sur du papier ou gravés sur une pièce de métal. La sécurisation des clés devient alors aussi simple que la sécurisation physique de la copie imprimée des clés bitcoin. Un ensemble de clés bitcoin imprimées sur papier s'appelle un "portefeuille papier" et de nombreux outils gratuits peuvent être utilisés pour les créer. Personnellement, je conserve la grande majorité de mes bitcoins (99 % ou plus) stockés sur des portefeuilles en papier, cryptés avec BIP-38, avec plusieurs copies enfermées dans des coffres-forts. Garder le bitcoin hors ligne est appelé *stockage à froid* (*cold storage*) et c'est l'une des techniques de sécurité les plus efficaces. Un système de stockage à froid est un système dans lequel les clés sont générées sur un système hors ligne (jamais connecté à Internet) et stockées hors ligne, soit sur papier, soit sur un support numérique, comme une clé USB.

### Portefeuilles matériels

À long terme, la sécurité des bitcoins prendra de plus en plus la forme de portefeuilles matériels inviolables. Contrairement à un smartphone ou à un ordinateur de bureau, un portefeuille matériel bitcoin n'a qu'un seul objectif: conserver les bitcoins en toute sécurité. Sans logiciel à usage général à compromettre et avec des interfaces limitées, les portefeuilles matériels peuvent offrir un niveau de sécurité presque infaillible aux utilisateurs non experts. Je m'attends à voir les portefeuilles matériels devenir la méthode prédominante de stockage de bitcoins. Pour un exemple d'un tel portefeuille matériel, voir le [Trezor](https://trezor.io/).

### Équilibrer les risques

Bien que la plupart des utilisateurs soient à juste titre préoccupés par le vol de bitcoins, le risque est encore plus grand. Les fichiers de données se perdent tout le temps. S'ils contiennent du bitcoin, la perte est beaucoup plus douloureuse. Dans le but de sécuriser leurs portefeuilles bitcoin, les utilisateurs doivent faire très attention à ne pas aller trop loin et finir par perdre le bitcoin. En juillet 2011, un projet bien connu de sensibilisation et d'éducation au bitcoin a perdu près de 7 000 bitcoins. Dans leur effort pour prévenir le vol, les propriétaires avaient mis en place une série complexe de sauvegardes cryptées. En fin de compte, ils ont accidentellement perdu les clés de cryptage, rendant les sauvegardes sans valeur et perdant une fortune. Comme cacher de l'argent en l'enterrant dans le désert, si vous sécurisez trop bien votre bitcoin, vous ne pourrez peut-être plus le retrouver.

### Risque de diversification

Porteriez-vous toute votre valeur nette en espèces dans votre portefeuille ? La plupart des gens considéreraient cela comme imprudent, mais les utilisateurs de bitcoins conservent souvent tous leurs bitcoins dans un seul portefeuille. Au lieu de cela, les utilisateurs devraient répartir le risque entre plusieurs portefeuilles bitcoin diversifiés. Les utilisateurs prudents ne conserveront qu'une petite fraction, peut-être moins de 5%, de leur bitcoin dans un portefeuille en ligne ou mobile comme "monnaie de poche". Le reste doit être réparti entre quelques mécanismes de stockage différents, tels qu'un portefeuille de bureau et hors ligne (stockage à froid).

### Multisig et gouvernance

Chaque fois qu'une entreprise ou un particulier stocke de grandes quantités de bitcoins, il doit envisager d'utiliser une adresse Bitcoin multisignature. Les adresses multisignatures sécurisent les fonds en exigeant un nombre minimum de signatures pour effectuer un paiement. Les clés de signature doivent être stockées dans un certain nombre d'endroits différents et sous le contrôle de différentes personnes. Dans un environnement d'entreprise, par exemple, les clés doivent être générées de manière indépendante et détenues par plusieurs dirigeants de l'entreprise, afin de garantir qu'aucune personne ne puisse compromettre les fonds. Les adresses multisignatures peuvent également offrir une redondance, où une seule personne détient plusieurs clés qui sont stockées à différents endroits.

### Capacité de survie

Une considération de sécurité importante souvent négligée est la disponibilité, en particulier dans un contexte d'incapacité ou de décès du détenteur de la clé. Les utilisateurs de Bitcoin sont invités à utiliser des mots de passe complexes et à garder leurs clés sécurisées et privées, sans les partager avec qui que ce soit. Malheureusement, cette pratique rend presque impossible pour la famille de l'utilisateur de récupérer des fonds si l'utilisateur n'est pas disponible pour les débloquer. Dans la plupart des cas, en fait, les familles des utilisateurs de bitcoins pourraient ignorer complètement l'existence des fonds en bitcoins.

Si vous avez beaucoup de bitcoins, vous devriez envisager de partager les détails d'accès avec un parent ou un avocat de confiance. Un régime de survie plus complexe peut être mis en place avec un accès multi-signatures et une planification successorale par l'intermédiaire d'un avocat spécialisé en tant qu'"exécuteur d'actifs numériques".

## Conclusion

Bitcoin is a completely new, unprecedented, and complex technology. Over time we will develop better security tools and practices that are easier to use by nonexperts. For now, bitcoin users can use many of the tips discussed here to enjoy a secure and trouble-free bitcoin experience.