# Bitcoin pour débutants 2024

Ce cours est conçu de sorte à vous faire passer du niveau débutant en la matière sans aucune connaissance, à l'utilisateur chevronné comprenant entièrement le fonctionnement et du pourquoi de l'existence de Bitcoin. Si vous avez déjà une certaine expérience sur le sujet, il y a de grandes chances que vous en apprendrez encore plus.

Ce que vous apprendrez:

- Qu'est-ce que la monnaie et son histoire.
- Pourquoi Bitcoin est important.
- Comment Bitcoin peut changer le monde.
- Comment Bitcoin protège votre argent.
- Comment acheter des bitcoins.
- Comment protéger soi-même vos bitcoins.
- Comment et où dépenser vos bitcoins.
- Comment recevoir des bitcoins.
- Comment maintenir votre vie privée.
- Qu'est-ce qu'un nœud et pourquoi ils sont importants.
- Qu'est-ce qu'une couche 2 et comment les utiliser.
- Qu'est-ce qu'un UTXO et comment les gérer.

***À la fin du cours, vous trouverez une liste de liens et de ressources qui vous aideront à en apprendre davantage et à mieux utiliser Bitcoin, ainsi que les ressources mentionnées dans ce cours. Il y aura aussi quelques codes QR Bitcoin pour faire un don si vous appréciez.***

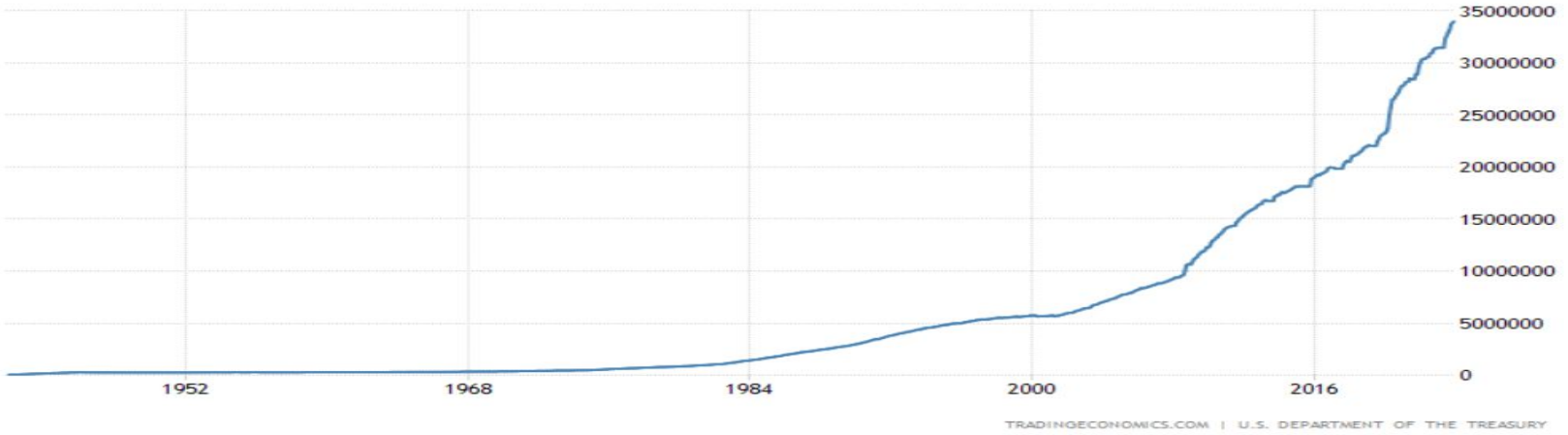
# Qu’est-ce que la monnaie?

- La monnaie est un bien commun utilisé pour l’échange de biens et de services.
- Vous convertissez votre temps et votre énergie par le travail en monnaie, que vous pouvez économiser et dépenser à une date ultérieure.
- Il y a eu de nombreuses formes différentes de monnaie tout au long de l’histoire: les coquillages et les pierres, l’argent et l’or, la monnaie fiduciaire papier et désormais la monnaie numérique comme Bitcoin.
- Il y a 6 propriétés principales pour qu’une monnaie soit bonne: durabilité, transportabilité, fungibilité, rareté, divisibilité et vérifiabilité.
- Avant l’invention de Bitcoin, l’or était la meilleure forme de monnaie disponible. C’est parce qu’il est très durable et ne peut pas être détruit. Il est fongible, ce qui signifie que chaque gramme d’or est tout autant précieux qu’un autre. Il est relativement rare car il nécessite de grandes quantités d’énergies pour en extraire plus et augmenter l’offre. Cependant, il a des problèmes de portabilité et de facilité de déplacement ou de transfert. Il a également du mal à être divisible, car vous devez le fondre en morceaux. Et enfin, ce n’est pas facilement vérifiable, à cause de métaux comme la pyrite (l’or des fous), ou de son alliage avec d’autres métaux et la nécessité d’un équipement spécialisé pour déterminer qu’il s’agisse bien d’or à 100%.

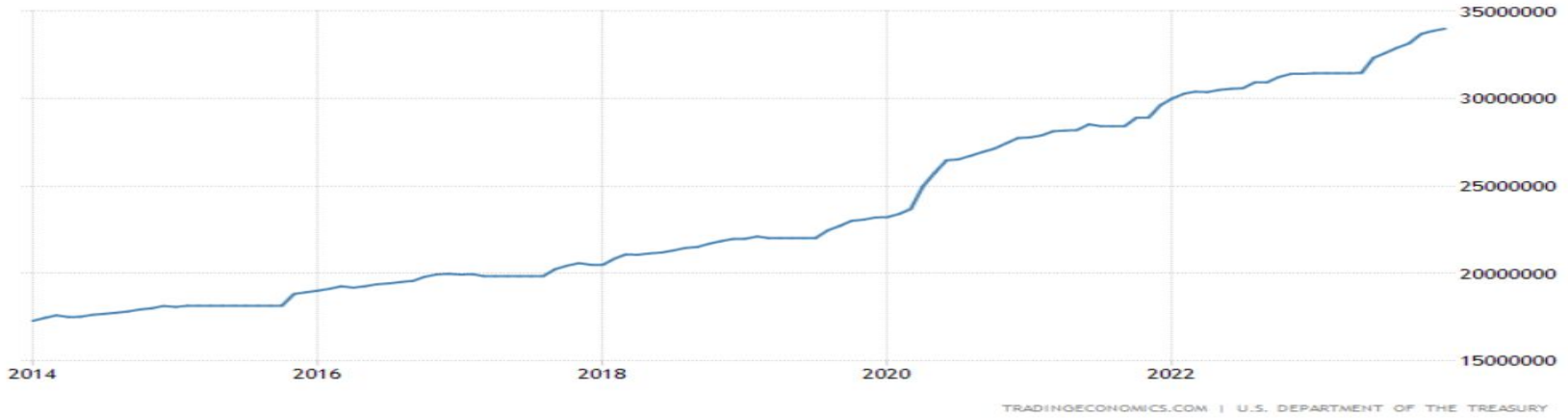
- C’est pourquoi la monnaie papier a été créée, pour augmenter ces 3 propriétés qui manquaient à l’or. Le papier est plus facile à transporter, il est plus divisible et il est plus facilement reconnaissable, même s’il peut encore être contrefait relativement facilement.
- Notre forme de monnaie actuelle s’appelle fiduciaire. Fiduciaire signifie “par décret”, ou “parce que je l’ai dit”. Cela signifie qu’un gouvernement dit qu’une chose est une monnaie et qu’il le défendra par une politique militaire et économique.
- Malheureusement, cela signifie que la monnaie fiduciaire est hautement centralisée et créée par une seule entité. Il s’agit essentiellement de donner un pouvoir absolu aux banques centrales et aux gouvernements qui émettent et créent la monnaie. Le pouvoir absolu corrompt absolument.
- La monnaie fiduciaire permet à l’émetteur de n’avoir aucune limite sur ses dépenses, autre que la perte de contrôle de la monnaie ainsi qu’une perte de confiance parmi les détenteurs de ladite monnaie.
- Cet effondrement monétaire se produit régulièrement partout dans le monde. Par exemple: Venezuela, Argentine, Zimbabwe, Liban, Nigeria, Allemagne (République de Weimar) et bien d’autres. Ces pays ont surimprimé leur monnaie pour payer leur dette et leurs dépenses publiques.

# Dette fiduciaire

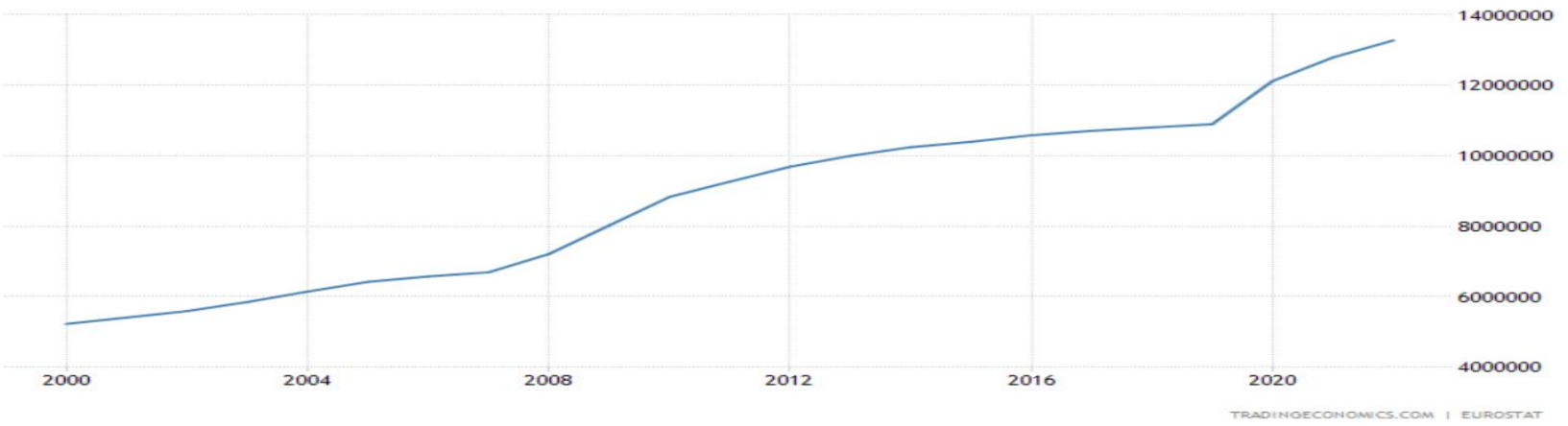
- Les gouvernements émettent des obligations à d'autres pays et à des particuliers pour financer leurs projets de dépenses. Une obligation est une promesse de payer des intérêts sur un prêt. Ainsi, si j'achète 100$ d'obligations américaines, je prête 100$ au gouvernement américain sur une période donnée et je recevrai des intérêts pendant que je détiens l'obligation. Ensuite, à la fin de la période de détention des obligations, je recevrai mes 100$. Donc, pour que je profite de ce commerce, le taux d'intérêt doit être supérieur au taux d'inflation de la monnaie. Parce que les 100$ que je recevrai à la fin valent moins en biens et services en raison de l'inflation.
- Cela signifie que les gouvernements qui vendent des obligations doivent payer des intérêts aux détenteurs d'obligations, et plus le taux d'intérêt est élevé, plus les remboursements sont élevés.
- Par exemple, les États-Unis ont plus de 34'000 milliards de dollars de dette en obligations. Et avec les taux d'intérêt actuels autours de 5%, ils doivent payer environ 1'500 milliards de dollars chaque année aux détenteurs d'obligations. Il convient toutefois de noter que le gouvernement américain achète sa propre dette avec de la monnaie imprimée, ce qui signifie qu'il reçoit ses propres paiements d'intérêts.
- Ils paient principalement cela en imprimant de la monnaie, ce qui entraîne une augmentation de l'inflation. Et plus l'inflation est élevée, plus le gouvernement augmente les taux d'intérêt, et donc plus les paiements annuels d'obligations sont élevés.
- Il s'agit d'un cercle vicieux, qui nécessite d'imprimer davantage de monnaie pour payer la dette, ce qui entraîne des montants plus élevés à rembourser. Et plus l'inflation est élevée, plus la situation de tous ceux qui utilisent la monnaie se détériore, en raison de l'augmentation du coût de la vie.




Ce graphique montre la dette des États-Unis depuis les années 1940. La dette actuelle dépasse 34’000 milliards de dollars.




Ce graphique montre les 10 dernières années de la dette américaine. Il a presque doublé en une décennie.




Ce graphique montre la dette de l'UE depuis 2000. La dette actuelle s'élève à environ 13’500 milliards d'euros.

# Pourquoi Bitcoin?

- Bitcoin a une offre fixe prédéterminée. Il n'y aura jamais plus de 21 millions de bitcoins, ce qui signifie qu'il s'agit d'un actif vraiment rare.
- La valeur du Bitcoin peut augmenter avec le temps, ce qui signifie que son prix est déflationniste pour les biens et services. Le coût de la vie peut baisser au lieu d'augmenter.
- Si un gouvernement qui utilise le Bitcoin veut dépenser plus d'argent, il doit l'obtenir auprès de ses citoyens ou en effectuant un travail récompensé par le Bitcoin. Ils ne pourraient pas simplement en créer davantage comme ils le peuvent avec la monnaie fiduciaire.
- Si vous savez que votre argent vaudra le même montant ou plus, mesuré en nourriture/abri/etc. vous pourrez alors planifier l'avenir de manière plus efficace et responsable. Vous n'avez plus besoin de dépenser de l'argent par crainte qu'il perde de la valeur. Cela a de nombreux effets profonds, tels que le fait de vivre de manière plus durable et d'inciter à épargner plutôt qu'à dépenser. Ceci est parfois appelé passer d'une préférence temporelle élevée, où vous souhaitez réfléchir davantage aux effets immédiats, à une préférence temporelle faible, où vous êtes plus patient et avant-gardiste.
- La valeur du Bitcoin peut augmenter pour toujours, tant que les humains qui les utilisent sont productifs et créent de la croissance économique. À long terme, cette croissance est estimée à environ 3 à 5 % par an en moyenne.
- Certains craignent la thésaurisation, mais si l'offre est vraiment limitée, alors les gens devront dépenser, simplement pour survivre, mais aussi pour tous les autres aspects de la vie normale qui nécessitent de dépenser de l'argent. De plus, nous pouvons toujours avoir des taux de prêt et d'intérêt. Si les gens accumulent un peu trop et que le marché a besoin de capitaux, le taux d'intérêt augmentera, incitant les gens à prêter leurs bitcoins à des fins productives.

- Bitcoin utilise une blockchain, où chaque bloc est enregistré dans l'ordre. Un bloc est un ensemble de transactions qui se produisent en moyenne toutes les 10 minutes. Ceci est similaire à un registre écrit indiquant quelle adresse possède quels bitcoins.
- N'importe qui peut auditer et lire ce registre, et savoir si une transaction est réelle et si un portefeuille possède réellement le bitcoin qu'il prétend revendiquer. Cela vous permet également de vérifier l'approvisionnement total en pièces.
- Bien qu'il soit pseudonyme, vous savez uniquement quelles adresses de portefeuille effectuent des transactions, pas les noms des propriétaires des portefeuilles ni aucune autre information personnelle. Ainsi, si je partage publiquement l'adresse de mon portefeuille, les gens peuvent suivre mes transactions et savoir combien j'ai, combien j'envoie et reçois.
- Ainsi, un gouvernement utilisant Bitcoin pourrait être amené à divulguer ses adresses de portefeuille et permettre à tout un chacun de suivre ses dépenses.
- Vous pourriez savoir exactement combien de bitcoins un pays possède réellement et combien il dépense. Contrairement au système actuel où la masse monétaire est estimée et où les actifs comme l'or sont inconnus. Bitcoin supprime la confiance nécessaire, vous pouvez simplement les auditer.
- Semblable à l'or et à la monnaie, vous pouvez conserver vous-même votre bitcoin. Cela signifie que vous êtes responsable de le stocker et que vous contrôlez votre propre argent.
- Cependant, il est numérique et non physique, ce qui signifie qu'il ne peut pas être physiquement volé. À moins que quelqu'un récupère votre clé privée, qui est comme un mot de passe pour dépenser votre bitcoin, que vous avez sauvegardée d'une manière ou d'une autre, peut-être sur du papier ou de l'acier. Cependant, vous pourriez potentiellement stocker votre clé privée uniquement dans votre cerveau, empêchant ainsi le vol et vous permettant de transporter vos bitcoins sans que personne ne le sache.

- Bitcoin est un système décentralisé, il n’est pas contrôlé par une seule entité mais par un vaste système de nœuds répartis dans le monde entier. Il existe des dizaines de milliers de nœuds, il est difficile de le savoir car ils peuvent être masqués à l'aide du réseau Tor ce qui améliore la sécurité des bitcoins en masquant l'emplacement d'un nœud. Un nœud est un ordinateur qui exécute le logiciel Bitcoin avec les règles de consensus convenues et conserve un enregistrement des transactions de la blockchain.

- Il est donc très difficile, voire impossible, pour un gouvernement de modifier les règles de Bitcoin. Comme changer l'offre de 21 millions ou changer la taille du bloc.

- Un autre avantage d’un système décentralisé est qu’il résiste à la censure. Personne ne peut vous empêcher d’effectuer une transaction ou vous empêcher d’utiliser votre argent. Vous ne pouvez pas vraiment avoir la liberté d’expression et la liberté de posséder des biens si vous n’avez pas la liberté d’effectuer des transactions. C’est le contraire d’une CBDC, qui est une monnaie numérique qui permettra au gouvernement de contrôler beaucoup plus votre vie, en limitant comment, quand et où vous pouvez dépenser votre argent.

- Le système permet cependant d'apporter des modifications si cela est absolument nécessaire, par exemple si un bug majeur était découvert. Il suffirait qu’une majorité d’utilisateurs acceptent les modifications et changent la version du logiciel.

- Bitcoin fonctionne sans autorisation, ce qui signifie que vous n'avez pas besoin de demander la permission à quiconque pour utiliser le réseau et stocker votre richesse en Bitcoin. Bien que le bitcoin soit principalement utilisé sur Internet, il existe des moyens de transférer du bitcoin en utilisant des ondes radio, un réseau de téléphonie mobile ou même par écrit.

- Plus de la moitié de la population mondiale vit sous des gouvernements autoritaires, où ils n'ont pas accès au même système bancaire que celui des pays développés. Bitcoin permet à ces personnes d'être leur propre banque et leur donne un outil pour quitter leur pays avec toutes leurs économies.

- Cela permet également le commerce entre des pays qui n'avaient auparavant aucun moyen de se payer.

- La sécurité améliorée et la difficulté de voler des bitcoins pourraient conduire à un monde avec moins de guerres, car il n'y aura peut-être plus d'argent à voler après avoir gagné une guerre, contrairement à des tas d'or ou d'argent liquide. L'incapacité d'un gouvernement à créer davantage de bitcoins peut également limiter la guerre, en limitant les sommes d'argent pouvant être dépensées pour les combats.

- Bitcoin est créé grâce à un processus appelé minage, ce processus encourage les énergies renouvelables et réduit le gaspillage d'énergie. Parce que si je crée un système minier qui utilise l'énergie solaire, par exemple, le coût de l'électricité peut devenir presque gratuit, ou je pourrais utiliser du gaz de torche qui sera gaspillé et le brûler pour produire du bitcoin, tout en transformant également le méthane en dioxyde de carbone moins nocif.

- Ce système permet de monétiser l'énergie partout dans le monde, il suffit d'avoir une connexion internet. Vous n'avez plus besoin de créer des tuyaux et des câbles pour envoyer l'énergie vers un endroit où se trouvent des gens, vous pouvez à la place extraire du Bitcoin et apporter l'argent aux gens.

- De plus, si un énergéticien décide de construire une nouvelle centrale électrique renouvelable par exemple, il pourra commencer à monétiser dès le premier jour de production d'électricité et ainsi gagner de l'argent 24h/24 et 7j/7. Auparavant, il fallait attendre que toutes les infrastructures soient construites pour pouvoir acheminer l'électricité vers des bâtiments où les gens peuvent la payer. Et peut-être qu'il n'y a pas assez de monde à proximité pour acheter toute votre énergie et que vous finissez par gaspiller de l'énergie, par exemple à midi dans le cas du photovoltaïque, lorsque la demande d'énergie est faible. Il existe une idée fausse selon laquelle le bitcoin est mauvais pour l'environnement, mais ce n'est pas vrai.

- ***Regardez cette vidéo pour découvrir pourquoi les gros titres selon lesquels le bitcoin est mauvais pour l'environnement sont faux :"FACT CHECK: Bitcoin Mining is BAD For The Climate!?"***

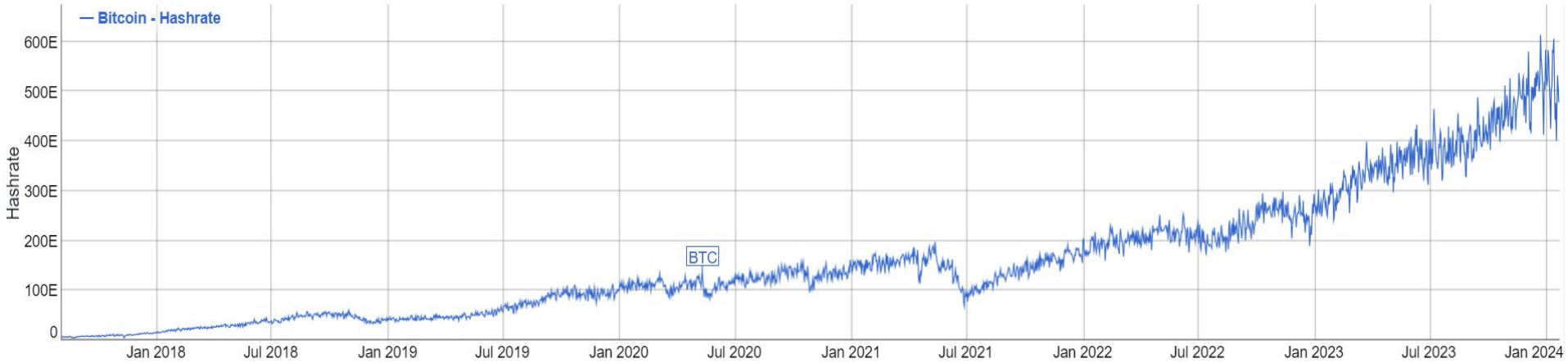
# Principes d’investissement

- Lorsque vous commencez à investir, vous devez réfléchir à certains conseils et évaluer votre niveau de tolérance au risque.
- Tout d’abord, n’investissez jamais plus que ce que vous pouvez perdre. Bien sûr, de nombreuses personnes investiront plus que cela, mais le montant dépendra de votre tolérance au risque. En gros, il vaut mieux ne pas investir un montant qui vous ruinerait financièrement s’il tombait à 0.
- Vient ensuite votre horizon temporel. Vous devez prévoir de conserver votre investissement pendant une longue période, plusieurs années, voire plusieurs décennies. Sinon, vous feriez du trading et vous risquez très probablement de perdre de l'argent au lieu de simplement le conserver à long terme. Le Bitcoin est un actif très cyclique et volatil. Historiquement il suit un cycle de 4 ans de hauts et de bas. Avec des chutes de 80 % ou plus. Sur la diapositive suivante, vous pouvez voir le graphique des prix historiques du Bitcoin et ses cycles très prononcés, en partie influencés par le calendrier de halving sur 4 ans.
- Traitez vos avoirs en bitcoins comme s’ils valaient bien plus, car ils pourraient bien le devenir un jour. N'attendez pas jusque-là pour prendre votre sécurité et votre confidentialité au sérieux.
- Évitez l’effet de levier, c’est un excellent moyen de perdre tout votre argent. Ne contractez pas de prêts pour acheter du Bitcoin ou n'utilisez pas d'instruments de négociation de contrats à terme à effet de levier. Nous recommandons également fortement de ne pas vendre à découvert le bitcoin, à moins que vous ne sachiez vraiment ce que vous faites et connaissiez les risques liés au trading d'un actif à forte volatilité.
- Déterminez si vous souhaitez acheter avec des sommes uniques ou par étalement des coûts en euro (DCA, Dollar Cost Average). Par exemple, vous avez 10’000 euro  à investir, achetez-vous 10’000 euro en une seule fois ou 100 fois une valeur de 100 euro, par exemple à intervalles quotidiens ou hebdomadaires. Si vous choisissez le DCA, portez une attention particulière à la leçon UTXO plus loin dans ce cours, car vous pouvez rencontrer des problèmes de frais lorsque vous retirez régulièrement de petits montants.

# Tableau des prix du Bitcoin 2012-2024

# Minage de bitcoins

- Le Bitcoin est créé par le « minage ». Des ordinateurs essayent de deviner un très grand nombre, tout en dépensant de l'énergie électrique.
- Toutes les 10 minutes, un nouveau bloc de transactions est ajouté à la blockchain, ce qui revient à ajouter une entrée dans un grand livre pour garder une trace de l'historique des transactions.
- Un seul ordinateur peut le faire toutes les 10 minutes, celui qui devine le bon numéro. Cet ordinateur est ensuite récompensé par la récompense de bloc, un montant prédéterminé de bitcoins, actuellement 3,125 bitcoins. Ils obtiennent également le total des frais payés par toutes les transactions de ce bloc.
- C’est ainsi que le bitcoin est créé, grâce à la récompense de bloc. Il cessera d’être créé une fois que les 21 millions de bitcoins auront été octroyés aux mineurs, bloc par bloc.
- En 2009, lorsque le bitcoin a été créé, la récompense par bloc était de 50 bitcoins. Ce montant est réduit de moitié tous les 210’000 blocs, soit environ tous les 4 ans. C'est ce qu'on appelle le halving (réduction de moitié), qui est préprogrammé.
- En avril 2024, la récompense fut réduite de 6,25 à 3,125 bitcoins. Les derniers satoshis, ou sats, seront créés vers 2140. Il s’agit de l’offre fixe prédéterminée.
- Les ordinateurs utilisés pour miner du Bitcoin nécessitent de grandes quantités d’électricité. Actuellement, la consommation énergétique totale du réseau est similaire à la consommation énergétique d’un petit pays.
- C'est ce qui sécurise le système. Plus la consommation d’énergie est importante, plus le système est sécurisé. En effet, pour créer une fausse transaction ou modifier l’historique des transactions, vous auriez besoin de plus de la moitié de la puissance de calcul actuellement exploitée. Cela représente un coût financier et énergétique aujourd’hui insurmontable.




- Le graphique ci-dessus montre le taux de hachage du réseau Bitcoin depuis 2018. Le taux de hachage est le nombre total de suppositions faites par tous les ordinateurs qui exploitent le Bitcoin. Actuellement, le taux de hachage est d'environ 500 Exahashes. Cela représente 500 000 000 000 000 000 000 de hachages (500 milliards de milliards de devinettes !) par seconde !

- Bitcoin a également un ajustement de difficulté, ce qui signifie qu'à mesure que de nouveaux ordinateurs commencent à miner, il deviendra plus difficile de deviner le nombre. Pour continuer à avoir la même probabilité de miner un bloc, vous devrez augmenter votre taux de hachage et votre dépense énergétique. Ou si la puissance de hachage quitte le réseau et qu'il y a moins d'ordinateurs qui exploitent, la difficulté diminuera, ce qui permettra aux mineurs restants de deviner plus facilement le nombre et à de nouveaux participants d'entrer dans la danse.

- Lorsque la récompense globale atteindra zéro vers 2140, la sécurité du réseau sera payée par les frais de transaction. Chaque transaction sur le réseau paie des frais, plus la demande d'envoi d'une transaction est élevée à un moment donné, plus les frais requis pour envoyer une transaction sont élevés. Ces frais combinés vont aux mineurs pour payer leurs coûts d'électricité, leurs coûts de matériel, etc. C'est ce que l'on appelle parfois le budget de sécurité, la valeur de la récompense globale plus les frais de bloc.

- ***La vidéo YouTube suivante fournit une description alternative du minage de Bitcoin avec des visuels et des graphiques : "What is Bitcoin Mining?"***

# Autoconservation (Self Custody)

- Bitcoin est un actif au porteur, ce qui signifie que si vous le possédez, il vous appartient.
- Comme mentionné précédemment, vous pouvez prendre possession du bitcoin, de la même manière que l'or ou l'argent liquide. Essentiellement, les clés privées sont ce que vous gardez et sécurisez.
- Une clé privée est utilisée pour signer une transaction, ce qui signifie que si vous possédez la clé privée, vous possédez le bitcoin connecté à cette clé privée. Il s'agit d'une chaîne de lettres et de chiffres de 256 octets (bits).
- ***Si vous souhaitez comprendre à quel point le cryptage 256 bits est sécurisé, regardez la vidéo YouTube liée ici : "How secure is 256 bit security?"***
- Cependant, en 2013, Bitcoin a été modifié pour faciliter le stockage, la mémorisation et la lecture d'une clé privée. Il s'agit de la liste de 12 ou 24 mots que vous écrivez lorsque vous créez un portefeuille et qui est généralement appelée phrase secrète de récupération. Ces mots proviennent d'un ensemble spécifique de 2048 mots anglais, qui peuvent être trouvés en ligne en recherchant « Liste de mots BIP39 ». Il est également bon d'avoir une copie papier de cette liste de mots stockée avec votre phrase de récupération secrète.
- Lors de la création d'une phrase de récupération secrète ou d'une clé privée Bitcoin, idéalement, cela devrait être fait hors ligne. Cela peut être fait de plusieurs manières. Vous pouvez utiliser un portefeuille matériel qui doit être conçu pour ne pas pouvoir se connecter à Internet, générer des nombres aléatoires et créer votre clé privée. Cependant, vous devez être sûr que les créateurs de l'appareil ont correctement programmé le générateur de nombres aléatoires. Une autre façon de créer une clé privée hors ligne sans faire confiance à personne d'autre qu'à vous-même consiste à lancer des dés ou à utiliser un jeu de cartes. Recherchez « comment créer une phrase de récupération secrète Bitcoin avec des dés/des cartes ». Si vous créez un portefeuille sur un appareil connecté à Internet, il est considéré comme un portefeuille actif, ce qui signifie qu'il est possible qu'il soit compromis, peut-être par un virus. Vous ne devez jamais prendre de photo ni stocker votre phrase de récupération secrète d'une manière connectée à Internet.

- Il existe de différents niveaux de sécurité que vous pouvez mettre en place pour stocker une phrase de récupération secrète. Le plus simple serait de l'écrire sur un morceau de papier et de le conserver quelque part dans votre maison. Cependant, vous pouvez également stocker la phrase de récupération secrète sur différents matériaux, tels que la pierre ou le métal. Cela augmente les chances que votre phrase de récupération survive à une catastrophe tels qu'un incendie ou une inondation. Cependant, cela augmente également potentiellement vos chances d'être volé, car la phrase est désormais difficile à cacher si le support est plus encombrant. Vous pouvez stocker une plaque de métal de plusieurs manières, dans un coffre-fort, dans un tiroir caché, dans un plancher ou un mur, ou même enfouie sous terre. Chacun a besoin d'un niveau de sécurité différent.

- Vous pouvez également conserver les phrases dans une enveloppe ou un récipient inviolable. Ainsi, vous savez simplement en regardant le sac si quelqu'un a vu votre phrase de récupération secrète, éventuellement un membre de votre famille ou une personne de confiance.

- Il y a des avantages et des inconvénients à avoir plusieurs copies de votre phrase de récupération secrète. L'un des avantages est que si votre maison brûle et que votre phrase est détruite, vous en avez toujours d'autres copies. Si vous perdez une copie, vous disposez également d'autres sauvegardes que vous pouvez récupérer ou si vous avez mal écrit l'une des phrases. Cependant, vous augmentez vos chances d'être volé, si vous avez 3 copies, vous devez maintenant garder 3 phrases différentes à l'abri des voleurs potentiels, l'ampleur du risque est entièrement subjective, pour certains, ce sera une très petite chance, et pour certains, une chance plus élevée. Personnellement, je pense que dans la plupart des cas, plusieurs copies présentent plus d'avantages que de risques.

- Une façon d'améliorer votre sécurité d'autoconservation consiste à utiliser plusieurs portefeuilles et à diviser votre bitcoin entre eux, de sorte que si l'un d'eux est perdu ou volé, vous ne perdez pas tout. Vous pouvez également créer un portefeuille leurre vide ou contenant une petite somme, à donner à un attaquant potentiel. Plus vous consacrez d'efforts à stocker la phrase de récupération secrète du leurre, plus elle sera convaincante. Il doit également être bien conservé s'il y a de l'argent dans le portefeuille.

# Types de portefeuilles

- Il existe de nombreux types de portefeuilles qui utilisent le réseau Bitcoin. Les exemples les plus importants sont : signature unique, signature multiple, portefeuille logiciel, portefeuille matériel et portefeuille Lightning.
- Un portefeuille à signature unique ne nécessite qu'une seule clé privée pour signer une transaction ou pour dépenser le bitcoin à l'intérieur du portefeuille.
- Un portefeuille multi-signature, ou multisig, nécessite plusieurs clés privées pour signer une transaction. Le nombre de clés nécessaires est prédéterminé dans une configuration N sur M. Par exemple, vous pourriez avoir un multisig 2 sur 3, qui aurait besoin de 2 clés privées sur 3 pour effectuer une transaction. Cela pourrait également être un 3 sur 5, 10 sur 15 ou même 25 sur 40, où 40 clés privées sont attribuées à un portefeuille, et vous auriez besoin de connaître 25 de ces clés pour dépenser à partir du portefeuille, vous pouvez choisir le nombre de clés.
- Un portefeuille logiciel est un portefeuille dans lequel les clés privées sont créées par le logiciel sur un téléphone ou un ordinateur tel qu'une application mobile, il est connecté à Internet et constitue donc un portefeuille chaud.
- Un portefeuille matériel est un appareil dédié qui crée et stocke votre clé privée hors ligne, sans connexion à Internet. Il est utilisé pour signer des transactions sans exposer votre clé privée à des menaces potentielles telles que des virus. Les portefeuilles matériels doivent être connectés à un portefeuille logiciel.
- Un portefeuille Lightning est un portefeuille de deuxième couche, qui vous permet d'utiliser le réseau Lightning. Il s’agit d’un réseau plus rapide et moins cher pour envoyer et recevoir des bitcoins. Nous y reviendrons plus en détail plus tard dans le cours.
- Idéalement, vous souhaitez utiliser des portefeuilles gratuits et open source.

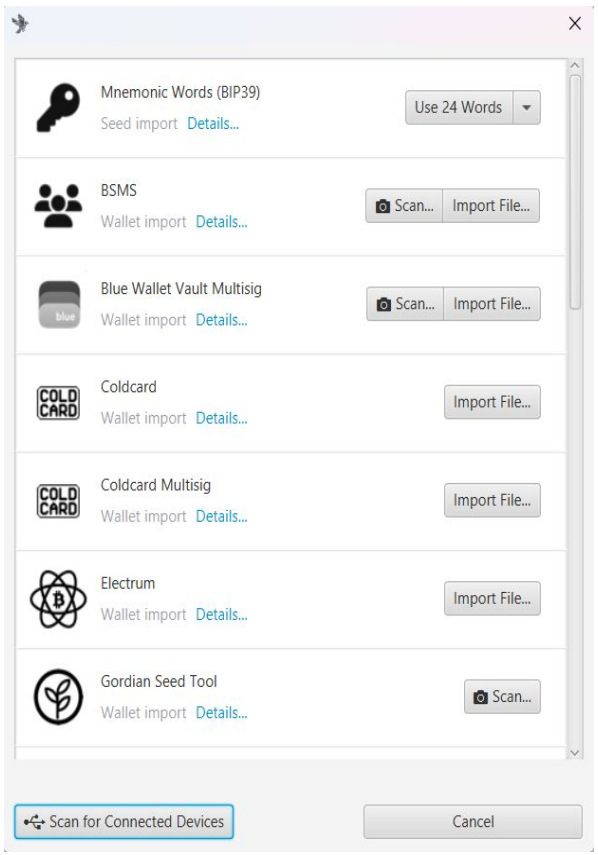
# Portefeuilles matériels

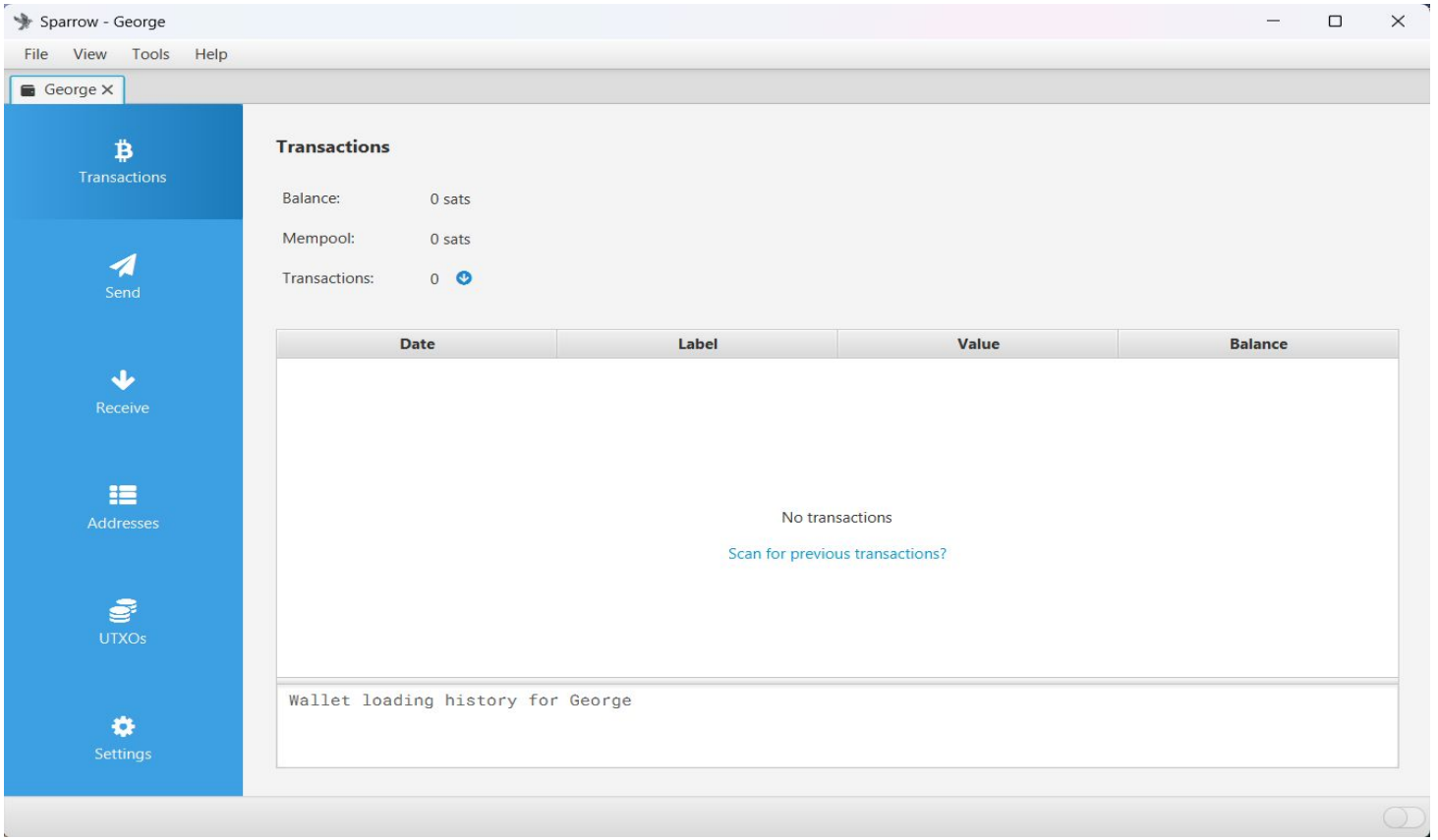

- Ci-dessus se trouvent les 4 portefeuilles matériels que je recommanderais le plus. De gauche à droite : Coldcard de Coinkite, Jade de Blockstream, Passport de Foundation et Bitbox de Bitbox Swiss.
- Ce sont tous des appareils très sécurisés, dotés de fonctionnalités très variées, notamment le multisig. Leurs prix varient, le Jade étant le moins cher.
- Ils ont tous un code open source, ce qui réduit la confiance que vous devez accorder à chaque entreprise et rend les appareils plus sécurisés.
- L'appareil ci-dessous s'appelle SeedSigner, il s'agit d'un portefeuille matériel entièrement gratuit et open source que vous pouvez créer vous-même. Vous achetez les pièces détachées puis installez vous-même le logiciel. Cela réduit la dépendance à l'égard des entreprises qui fabriquent les autres portefeuilles matériels, mais c'est plus complexe et peu convivial pour les débutants.

# Portefeuilles logiciels

- Il existe de nombreux portefeuilles logiciels Bitcoin disponibles. Je me concentrerai sur quelques-uns de mes préférés que je recommanderais.
- Il existe 2 autres catégories dans lesquelles vous pouvez placer des portefeuilles : le portefeuille en auto-garde et le portefeuille de garde.
- Le portefeuille en auto-garde est l'endroit où vous détenez vos propres clés privées et personne d'autre n'a accès à votre bitcoin. C'est le type de portefeuille dans lequel vous devez stocker la plupart, sinon la totalité, de vos bitcoins. La plupart des portefeuilles qui seront abordés dans ce cours sont auto-conservateurs.
- Le portefeuille de garde est l'endroit où vous n'avez pas accès aux clés privées, mais elles sont détenues par la société qui a créé le portefeuille. Cela signifie que l'entreprise a le contrôle total de votre bitcoin et peut potentiellement le voler ou limiter la façon dont vous le dépensez. La plupart des bourses, comme Coinbase ou Binance, vous offrent un portefeuille de garde. Je vous recommande de ne pas stocker beaucoup d'argent dans ces types de portefeuilles.
- Les portefeuilles que je recommande le plus sont : Sparrow Wallet (ordinateur de bureau), Electrum (ordinateur de bureau/Android), Blockstream Green (Mobile et ordinateur de bureau). Ce que vous choisirez d'utiliser dépendra de vos préférences personnelles et des fonctionnalités dont vous avez besoin ou du portefeuille matériel dont vous disposez. Nous examinerons chacun de ces portefeuilles plus en détail au cours des prochaines diapositives.
- Si vous n'utilisez pas de portefeuille matériel connecté à votre portefeuille logiciel, il est alors plus sûr d'utiliser un portefeuille mobile, car les systèmes d'exploitation mobiles sont moins sensibles aux virus et autres vulnérabilités.

# Sparrow



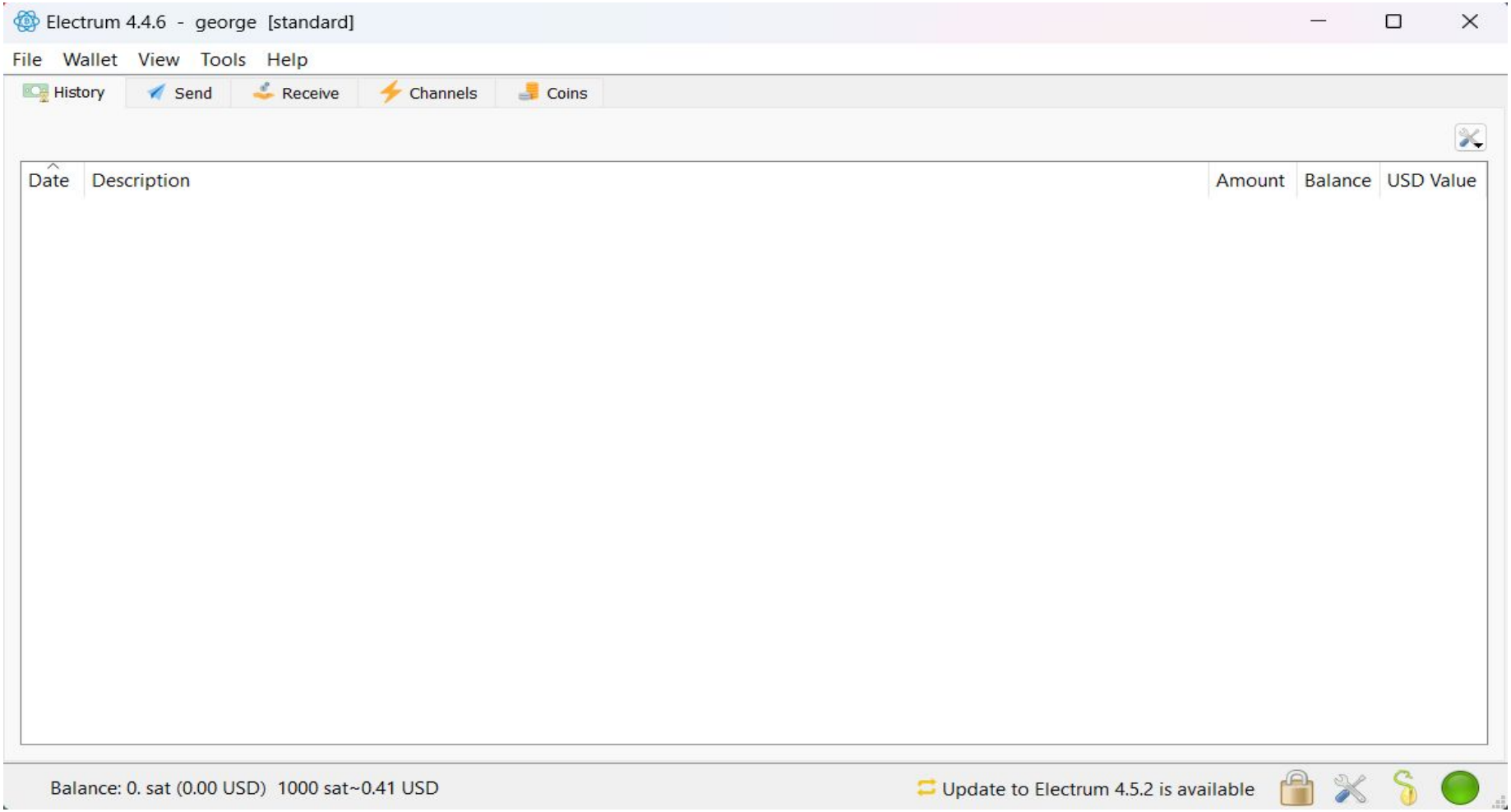




- Sur la droite se trouve la page d'accueil du portefeuille Sparrow, où vous pouvez voir l'historique des transactions et accéder aux pages d'envoi, de réception, d'adresses, d'UTXO et de paramètres.

- Sur la gauche se trouvent quelques-unes des façons dont vous pouvez utiliser Sparrow, comme importer une phrase de récupération secrète, connecter un portefeuille matériel comme Coldcard & Jade ou lier un portefeuille Electrum.

- Sparrow est l'un des portefeuilles les plus riches en fonctionnalités, vous permettant de faire beaucoup de choses. Tel que Whirlpool CoinJoins, signer des messages, RBF/CPFP, gestion UTXO, effectuer des paiements par lots et accéder au testnet Bitcoin. Il est également entièrement open source.

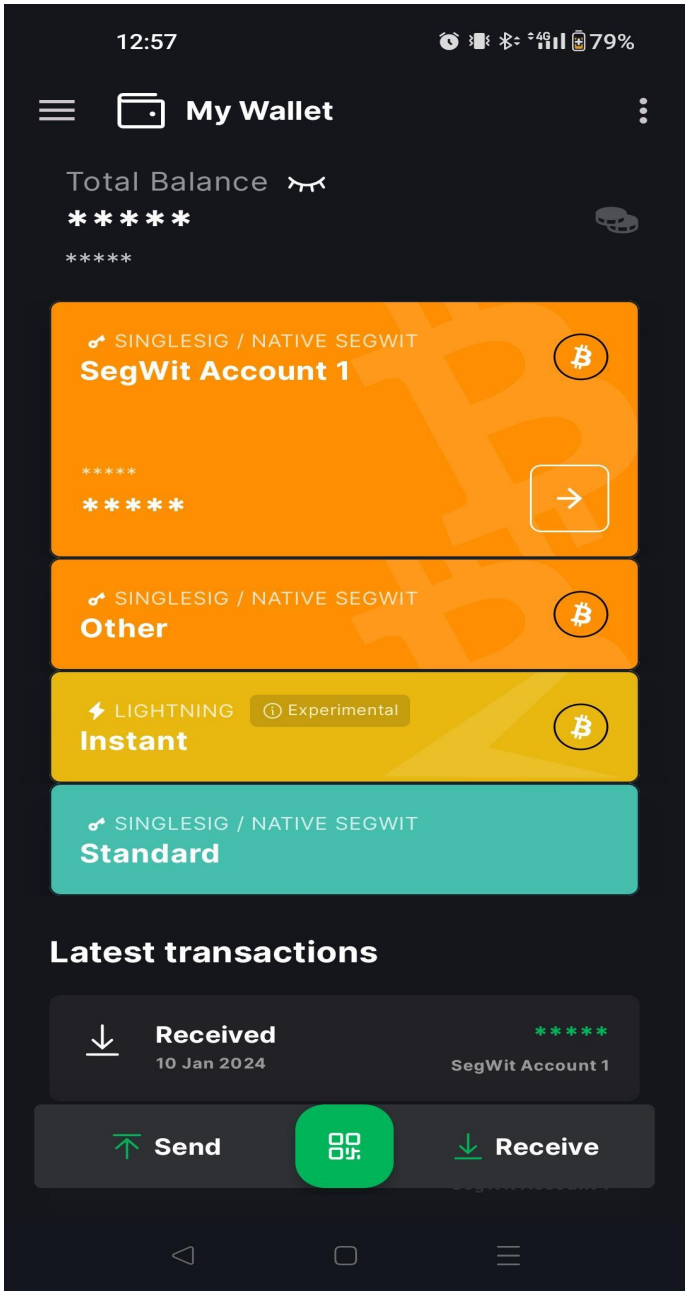
# Electrum



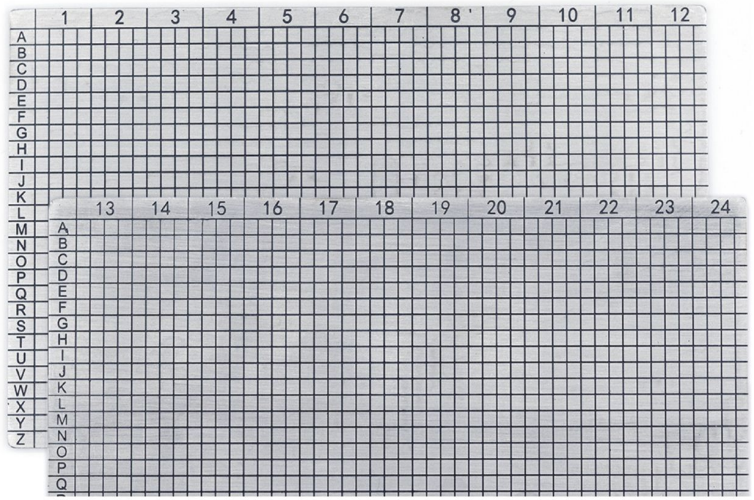

- Electrum est un autre portefeuille riche en fonctionnalités, disponible sur ordinateur et mobile Android. C'est l'un des plus anciens portefeuilles Bitcoin, créé en 2011 et entièrement open source.
- Il possède bon nombre des mêmes fonctionnalités que Sparrow, ainsi qu'un accès au réseau Lightning et la possibilité de créer des canaux.
- Il peut également être utilisé avec de nombreux portefeuilles matériels et pour le multisig.

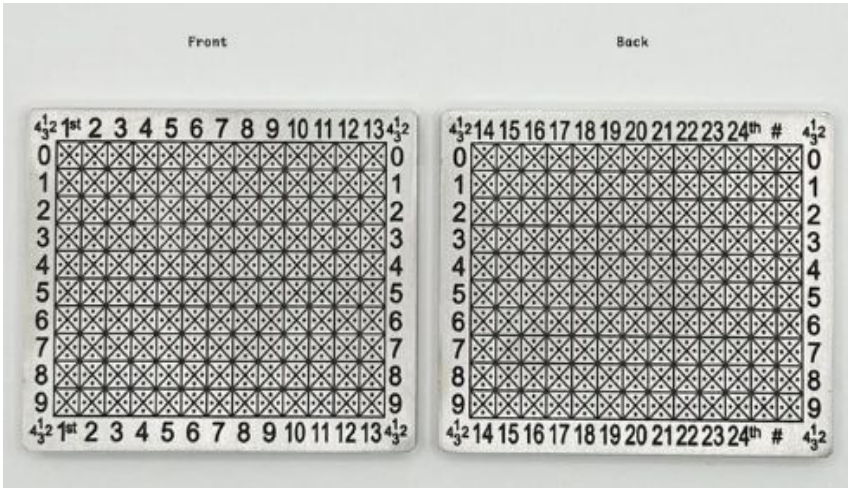
# Blockstream Green

- C'est probablement mon portefeuille préféré. Il possède une interface simple et claire sur mobile et sur ordinateur.
- Il est conçu pour fonctionner de manière transparente avec le portefeuille matériel Jade, également de Blockstream.
- Il ne dispose pas d'autant d'outils que Sparrow et Electrum, tels que CoinJoin ou les paiements groupés, mais pour la plupart des utilisateurs, il possède toutes les fonctionnalités dont vous avez besoin.
- Green vous permet également d'accéder au réseau Lightning et au réseau liquid, ce sont les couches 2.
- Le réseau liquid a été créé par Blockstream, c'est donc le meilleur portefeuille pour interagir avec liquid.
- La version de bureau possède des fonctionnalités supplémentaires que la version mobile n'a pas, comme la gestion UTXO.
- Tout comme Sparrow et Electrum, Green Wallet est entièrement open source.



# Seed Phrase Backups




- Voici 3 exemples de solutions de sauvegarde de phrases de récupération secrète, toutes en acier.
- En haut à gauche se trouve le SEEDPLATE, qui comporte une grille de 12 mots de chaque côté et utilise les 4 premières lettres de chaque mot dans une phrase de récupération secrète.
- En haut à droite se trouve Punchplate mini, il comporte également 12 mots de chaque côté. Cependant, au lieu des 4 premières lettres de chaque mot, il utilise 4 chiffres pour identifier le mot dans la liste de mots BIP39.
- L'image finale est la capsule Cryptosteel, qui utilise des pièces de type rondelle pour chaque lettre et est stockée à l'intérieur d'un tube en acier.

- Les sauvegardes métalliques ne sont pas le seul moyen de stocker votre phrase de récupération secrète, mais je pense qu'elles constituent actuellement le meilleur moyen. La pierre peut également être utilisée, mais elle n'est pas aussi solide que l'acier et peut être plus grosse.

- Vous pouvez également stocker votre phrase de récupération secrète sur un morceau de papier, mais il existe plusieurs raisons pour lesquelles vous ne devriez pas utiliser le papier comme solution de stockage à long terme. Premièrement, en cas de dégâts d'incendie, le papier ne survivrait pas, et deuxièmement, les dégâts d'eau provoqués par une inondation ou l'éclatement d'un tuyau détruiraient également le papier. Même un peu de moisissure ou d'humidité pourrait ruiner la lisibilité de la phrase de départ. De plus, l'encre peut s'estomper et couler avec le temps, ce qui rend la phrase encore une fois illisible. Le trait peut tacher s'il est touché ou être effacé par friction. Un morceau de papier peut également être pris pour un déchet et jeté.

- Vous devrez également décider si vous souhaitez une seule sauvegarde de votre phrase de récupération secrète ou si vous souhaitez plusieurs copies. Il y a des avantages et des inconvénients à avoir plusieurs copies.

- Le principal avantage des copies multiples est la redondance. Vous pourriez perdre, détruire ou même enregistrer de manière incorrecte l'une de vos phrases de départ et disposer encore d'une ou plusieurs copies supplémentaires sur lesquelles vous appuyer.

- Le principal inconvénient des copies multiples est le risque accru de vol. Si vous avez 3 copies de phrase de départ au lieu d'une, vous avez essentiellement triplé vos chances de vous faire voler votre phrase de récupération secrète. Ce risque de vol peut cependant être très faible, selon la manière et l'endroit où vous stockez les phases.

- Je pense que pour la plupart des gens, cela vaut la peine d'en avoir 2 ou 3 exemplaires au total. Chaque copie doit être stockée séparément, idéalement dans des bâtiments différents ou potentiellement même dans des villes/pays différents. Vous ne voulez pas qu'un seul incendie ou inondation affecte plus d'une copie de votre phrase de récupération secrète.

- ***Si vous souhaitez faire plus de recherches sur les différents types de sauvegardes de graines d'acier, regardez la vidéo suivante : "Steel Backups Video" et consultez ce lien de Jameson Lopp : "Lopp"***

# Multisignature

- Nous avons brièvement mentionné le multisig plus tôt, mais cela vaut la peine d'entrer plus en détail sur ce que c'est et si c'est un bon choix pour vous.
- Multisig augmente la sécurité de votre portefeuille, en exigeant plusieurs clés pour signer une transaction.
- Ces clés privées/phrases de récupérations secrètes supplémentaires peuvent être stockées dans des emplacements complètement différents, ce qui rend très difficile la dépense du bitcoin dans votre portefeuille. Le but est de rendre difficile, voir presque impossible, le vol de votre bitcoin par une attaque/ un voleur.
- Par exemple, vous pourriez avoir un multisig 2 sur 3, où chaque clé est stockée dans une ville ou même un pays différent. Donc, pour qu'un attaquant vous vole, il devrait se rendre à 2 des 3 emplacements pour trouver les clés. L'une de ces clés pourrait même potentiellement se trouver à l'intérieur d'une banque, dans un coffre-fort, ce qui serait très difficile à prendre pour un attaquant.
- Si vous possédez des clés dans différents pays, vous disposez également d'une protection contre un gouvernement qui souhaite prendre votre bitcoin. Ils devraient coopérer avec les autres pays dans lesquels vos phrases de départ sont stockées pour que les deux gouvernements puissent mettre la main sur vos clés, et cela en supposant qu'ils puissent trouver où vous les avez cachées.
- Vous pouvez également utiliser un multisig pour partager la garde d'un portefeuille avec d'autres personnes. Par exemple, vous êtes un groupe de 3 personnes qui possèdent une entreprise ensemble et vous souhaitez conserver vous-même votre bitcoin sans en donner le contrôle à un seul membre du groupe. Vous pouvez chacun avoir une clé pour un multisig 2 sur 3, et pour que le bitcoin soit dépensé, vous avez besoin de la signature de 2 des propriétaires d'entreprise. Il y a moins de chances que deux personnes travaillent ensemble pour vous voler qu'une seule personne vous vole.

- Un autre avantage du multisig est que vous pouvez perdre l’une des clés tout en conservant accès à votre portefeuille.

- Cependant, le multisig présente certains inconvénients.

- Vous devez stocker plus de données, avec un portefeuille simple, vous n'avez qu'à masquer et sécuriser une seule phrase de récupérations secrète, avec un multisig, vous avez désormais plusieurs phrases de récupérations secrète à sécuriser. Mais ce n'est pas tout, vous devez également stocker le fichier de configuration du portefeuille multisig ou les clés publiques xpub/ypub/zpub de chaque portefeuille. En effet, vous ne pouvez pas recréer et récupérer le multisig sans les clés privées et publiques.

- Ainsi, pour un multisig 2 sur 3, vous devrez stocker 3 phrases de départ différentes, et à côté de chaque phrase de départ, vous aurez besoin de 3 clés publiques, une de chacun des portefeuilles. Ces clés publiques ne sont pas non plus au format de mots anglais comme les phrases de départ, il s'agit d'une longue chaîne de lettres et de chiffres, ce qui rend leur stockage plus difficile. Je crois que cela s'améliorera à l'avenir.

- Un autre inconvénient du multisig est qu'il est plus cher à dépenser, les frais pour un multisig sont environ 70 % plus élevés que pour un portefeuille avec une seule signature. Plus tard, lorsque nous discuterons d'UTXO, vous comprendrez pourquoi il s'agit d'un problème sérieux pour certaines personnes.

- En utilisant multisig, vous augmentez également la complexité de votre configuration d'auto-garde. Cela pourrait signifier qu’il est trop difficile pour vos héritiers de récupérer et d’hériter de votre bitcoin lorsque vous êtes parti.

- En fin de compte, je ne recommande pas vraiment le multisig à la plupart des gens, à moins que vous ne disposiez d'une très grande quantité de bitcoins et que vous compreniez parfaitement le fonctionnement du multisig et ses compromis. Un portefeuille à signature unique est probablement suffisamment sécurisé pour la plupart des gens. Multisig doit principalement être utilisé par les grandes entreprises, les entreprises, les gouvernements et les dépositaires.

- Il existe des solutions collaboratives multisig, comme casa ou unchained. C’est là que l’entreprise détient l’une des clés et est en mesure de vous aider à signer des transactions plus facilement et également à vous aider à récupérer. Vous pourriez avoir un multisig 2 sur 3, où 2 des clés sont contrôlées par vous, potentiellement avec 2 portefeuilles matériels, et la troisième clé est détenue par le dépositaire, par exemple Unchained.

- Vous n'avez plus besoin d'aller chercher vos deux clés si vous souhaitez effectuer une transaction, vous n'en avez besoin que d'une seule et de la clé fournie par le dépositaire, généralement via une application ou un site Web.

- Lorsque vous utilisez l'un de ces services, vous n'avez plus nécessairement besoin de stocker les clés publiques, car le dépositaire les stocke généralement pour vous. Cependant, vous comptez sur leur existence dans le futur.

- Il existe également une fonction de sécurité appelée phrase secrète, qui est un mot supplémentaire que vous pouvez attacher à votre clé privée/phrase de récupération secrète. Ainsi, pour effectuer une transaction, vous aurez besoin de votre clé privée de 12 à 24 mots, plus le mot supplémentaire. Ce mot supplémentaire peut provenir de n'importe quoi, pas seulement de la liste de mots BIP39. En fait, c'est comme un multisig 2 sur 2. Personnellement, c'est un très bon moyen d'obtenir une sécurité supplémentaire, car vous n'avez besoin de stocker qu'un seul mot supplémentaire, mais il peut être complètement séparé de votre clé privée, vous offrant ainsi une sécurité supplémentaire contre le vol ou l'extorsion. Mais vous augmentez légèrement le risque d'erreur humaine si vous oubliez le mot et ne le stockez pas en toute sécurité.

- Si vous souhaitez supprimer tous les points de défaillance uniques de votre configuration d'auto-garde, je vous recommande d'utiliser une phrase secrète. Cependant, vous devriez étudier davantage cette fonctionnalité avant de l'utiliser.

# Planification successorale

- Nous allons maintenant vous expliquer comment créer un plan d'héritage pour votre bitcoin de garde à signature unique. Cela doit être distinct de toute instruction visant à récupérer des actifs sur des comptes de dépôt, tels qu'une banque, une maison de courtage ou une bourse.

- Vous ne savez jamais ce qui va se passer, quand vous mourrez ou subirez une lésion cérébrale par exemple. Il est donc bon de se préparer avec des instructions détaillées sur la façon de récupérer votre bitcoin pour vos héritiers ou vos proches.

- Étape 1 : Vous devez choisir une ou plusieurs personnes en qui vous avez confiance pour connaître l'emplacement de votre ou vos phrases de récupération secrète. **Cela ne doit être discuté qu'en personne, hors ligne.** Vous devriez également essayer d'identifier une ou plusieurs personnes qui ont une certaine connaissance du Bitcoin et en qui vous avez suffisamment confiance pour aider vos héritiers dans le processus de récupération. Cependant, indiquez clairement que ces personnes n'ont pas besoin de voir les mots de la phrase de récupération secrète, elles peuvent simplement dire à l'héritier où saisir les mots dans le portefeuille Bitcoin.

- Étape 2 : Écrivez des instructions sur la manière de lire la phrase de récupération secrète sur la plaque d'acier et de la traduire en 12/24 mots. Celles-ci doivent être stockées avec chaque phrase de récupération secrète ainsi que dans le cadre du plan d'héritage global. **Encore une fois, il ne doit pas inclure d'informations sur l'emplacement de la phrase de récupération secrète ou sur la phrase elle-même.** Par exemple, si vous avez une plaque à phrase en grille en acier, vous devez décrire comment lire chaque lettre ou chiffre dans le motif de grille, chaque conception de plaque en acier est unique, alors soyez précis lors de la description. Chaque sauvegarde de récupération secrète doit également contenir une copie de la liste de mots BIP39.

- Étape 3 : Vous devrez ensuite rédiger des instructions sur la façon de télécharger un portefeuille Bitcoin, avec plusieurs exemples de portefeuilles. Je recommande le Sparrow, Electrum ou Blockstream green. Je recommanderais de le faire sur un portefeuille d'ordinateur de bureau car ils ont plus de fonctionnalités, mais un portefeuille mobile convient également. En fait, si l'héritier n'utilise pas de portefeuille matériel, il serait alors plus sûr d'utiliser un portefeuille mobile.

- Étape 4 : Idéalement, la personne qui hérite du bitcoin aurait accès à un portefeuille matériel ou l'achèterait avant de le récupérer, afin de ne pas avoir à exposer la phrase de départ à un appareil connecté à Internet. Ceci est cependant facultatif.

- Étape 5 : Vous avez ensuite besoin d'instructions pour guider la personne tout au long de la récupération de la phrase de récupération secrète. Où saisir les clés et où ne pas les saisir (avertissements d'arnaque). Vous devrez détailler à quel point il est important de garder la phrase de départ privée et sécurisée. Vous devrez également expliquer comment effectuer une transaction vers un nouveau portefeuille au cas où l'ancien serait potentiellement compromis, inclure des descriptions des frais, comment savoir combien de frais ils paient en sats/VB et quels sont les frais de réseau moyens actuels en utilisant un site comme Mempool. Puis enfin, décrire les adresses de réception Bitcoin, où les trouver et à quoi elles pourraient ressembler. Espérons qu'à l'avenir, les écoles pourront enseigner aux gens le Bitcoin et comment l'utiliser, ou vous pourrez enseigner vous-même à vos héritiers/proches, en utilisant peut-être ce cours. De cette façon, vos instructions d'héritage n'ont pas besoin d'inclure autant d'informations.

- Étape 6 : Vous devez également expliquer comment envoyer le bitcoin sur un échange et comment le vendre contre des monnaies fiduciaires comme £, $, € ou CHF. J'espère qu'ils n'auront pas besoin de le faire, mais nous ne connaissons pas l'avenir.

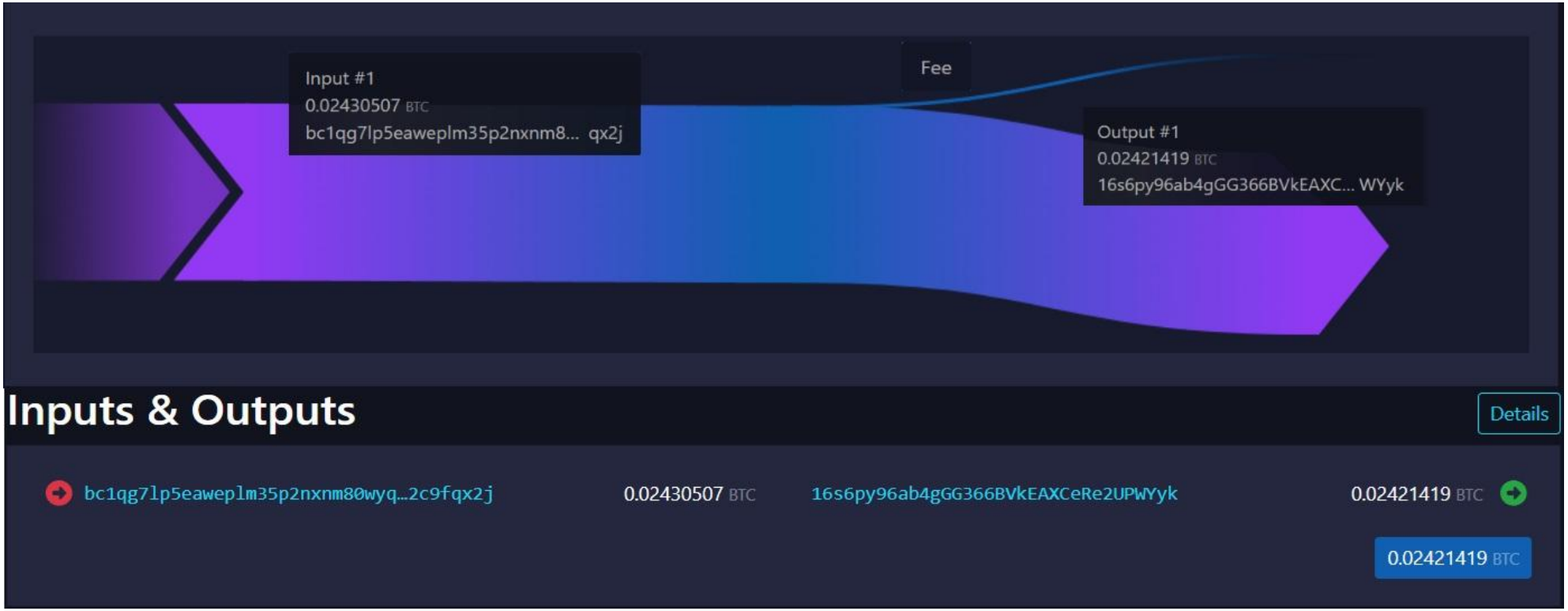
- Étape 7 : Je recommande fortement soit d'inclure des liens vers des guides vidéo YouTube pour récupérer un portefeuille, effectuer des transactions et comment les vendre sur un échange, soit de réaliser les vidéos vous-même.

- Étape 8 : Ces instructions d'héritage doivent être soigneusement organisées dans un document numérique et stockées à plusieurs endroits, éventuellement enregistrées sur un compte de stockage cloud ou envoyées par courrier électronique aux héritiers. Vous pouvez également les conserver sur une carte SD ou une clé USB et les stocker dans un coffre-fort personnel ou même dans un coffre-fort bancair. Un avocat pourrait également avoir des copies de ces instructions avec votre testament, qui devrait également indiquer à vos héritiers qui obtient quoi. Vous devriez également avoir des copies papier de vos instructions de succession. **Ces instructions ne doivent contenir aucune information sur l'emplacement des phrases de récupération secrète ou sur le contenu des phrases de départ elles-mêmes.**

# UTXOs

- UTXO est un acronyme qui signifie Unspent Transaction Output(Transaction de sortie non-dépensée). La transaction est souvent abrégée en TX, d'où Unspent TX Output. BTC est une manière abrégée d'écrire Bitcoin.

- Lorsque vous effectuez une transaction sur le réseau Bitcoin, celle-ci est constituée d'entrées et de sorties. Vous trouverez ci-dessous un organigramme qui montre une transaction simple d'un portefeuille à un autre. Ces diagrammes peuvent être consultés en allant sur ***Ces diagrammes peuvent être consultés en allant sur [mempool.space](mempool.space)***




- Sur la gauche, vous pouvez voir l'entrée de 0,0243 BTC, ce morceau de bitcoin était un UTXO, il est ensuite dépensé, ce qui signifie qu'il ne s'agit plus d'une sortie TX non dépensée, c'est maintenant une entrée.

- Sur la droite se trouve la nouvelle sortie, il s'agit maintenant d'un UTXO nouvellement créé. D'une valeur de 0,0242 BTC. La valeur a légèrement diminué, car un petit montant a été prélevé comme frais de réseau pour payer les mineurs. Vous pouvez voir cette fine ligne marquée en haut de l'organigramme.

- Voici un exemple, imaginez que vous avez 1 BTC dans un portefeuille et qu'il est composé de 10 UTXO d'une taille de 0,1 BTC chacun. Si vous souhaitez envoyer la totalité du 1 BTC, vous devrez envoyer les 10 UTXO. Cela signifie que vous disposez de 10 entrées pour la transaction de 0,1 BTC chacune et que vous aurez 1 sortie de 1 BTC moins les frais pour payer les mineurs, qui sont désormais un nouvel UTXO. Plus la sortie des frais elle-même.

- Plus le nombre d'entrées et de sorties dans une transaction est important, plus la taille des données de la transaction, mesurée en octets virtuels, est grande. Et plus il y a d'octets virtuels dans une transaction, plus les frais de réseau seront élevés. Toutefois, les entrées coûtent beaucoup plus cher que les sorties.

- Si vous souhaitez effectuer une transaction inférieure à la taille de votre UTXO, elle aura 1 entrée et 3 sorties. Voici un autre exemple avec un UTXO de 1 BTC essayant de dépenser seulement 0,5 BTC, l'entrée serait de 1 BTC et les sorties seraient un UTXO de 0,5 BTC pour la personne que vous souhaitez payer, une sortie des frais allant aux mineurs, puis une UTXO qui représente 0,5 BTC moins les frais, revenant dans votre portefeuille sous forme de change. Ce processus d'obtention de monnaie est automatique et ne peut pas être bloqué par le destinataire.

- Ceci est similaire au fonctionnement de l'argent liquide. Vous stockez l'argent liquide sous forme de coupures, comme les billets 5/10/20. Si vous avez 5 billets de 20 $, totalisant 100 $, et que vous souhaitez dépenser 60 $, vous devez remettre 3 billets de 20 $. De la même manière, si vous avez 3 UTXO d'une valeur de 20 $ chacun et que vous souhaitez acheter quelque chose pour 60 $, vous devrez envoyer les 3 UTXO. Si vous souhaitez dépenser seulement 10 $, vous remettez 20 $ et récupérez 10 $ en monnaie.

- Si vous possédez un UTXO très petit, il peut être peu rentable de le dépenser, en raison des frais de transaction, voire impossible à dépenser. Si vous avez un UTXO à 5 $ et que son envoi coûte 5 $ de frais, alors il est essentiellement sans valeur ou verrouillé jusqu'à ce que les frais diminuent.

- À l'avenir, il est très probable que les frais moyens requis pour envoyer une transaction augmentent. Comme indiqué précédemment, les frais devront à eux seuls financer le budget de sécurité.

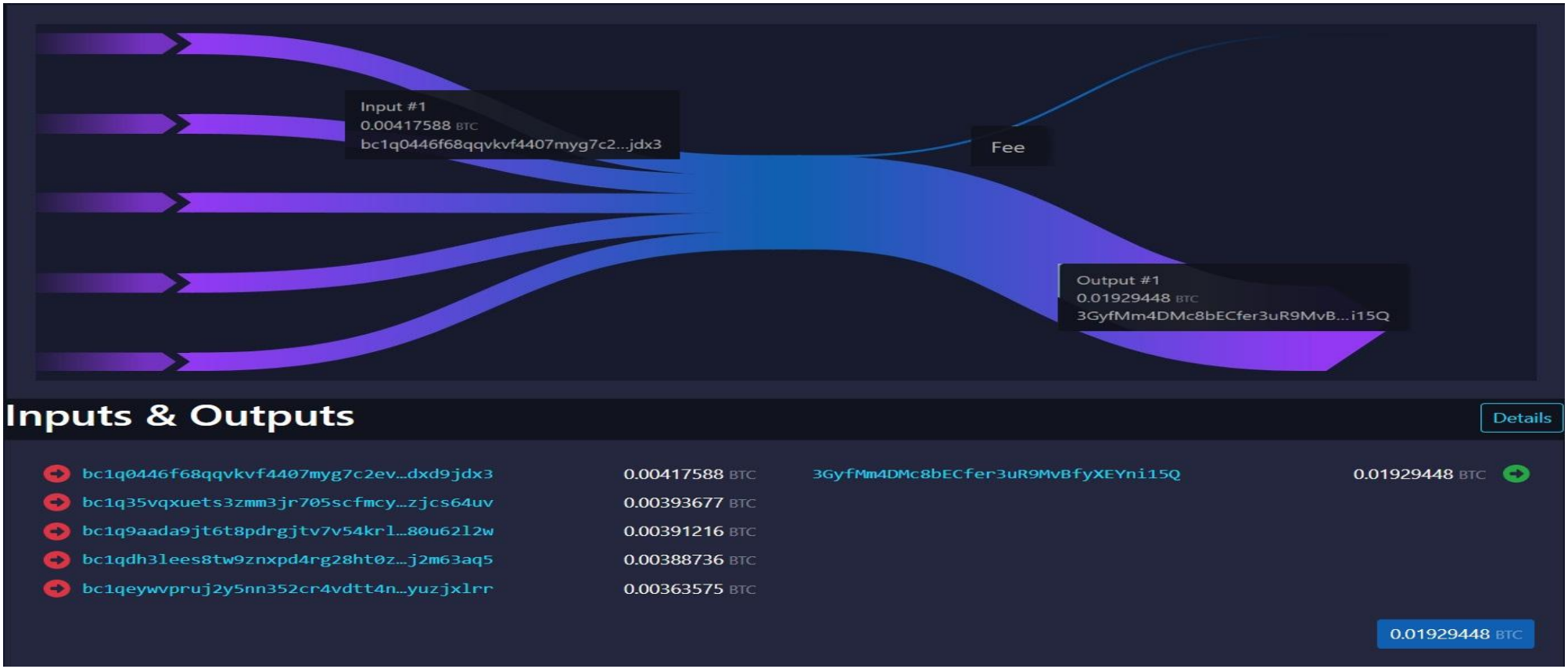
- Ainsi, comme les frais sont susceptibles d'augmenter, il est important de ne pas avoir d'UTXO de petite taille. Parce qu'ils pourraient potentiellement devenir sans valeur ou très coûteux à dépenser. Si jamais vous devez effectuer un paiement qui nécessite que plusieurs de vos UTXO soient combinés et utilisés comme entrées, cela utilisera plus d'octets virtuels et coûtera donc beaucoup plus cher qu'une transaction avec une seule entrée.

- Un montant minimum que je recommanderais pour les UTXO de stockage sur portefeuille matériel est de 0,01 BTC ou 1 million de satoshis. 1 BTC est composé de 100 millions de satoshis, tout comme 1 $ est composé de 100 cents. Mais plus l'UTXO est gros, mieux c'est, en ce qui concerne la protection future de votre bitcoin contre la hausse des frais. Le seul inconvénient est que vous pouvez obtenir moins de confidentialité en attachant tous vos bitcoins à une seule adresse bitcoin. Cependant, il existe des solutions à ce problème dont nous discuterons plus tard. Bien sûr, certaines personnes ne pourront peut-être pas se le permettre, auquel cas vous devrez décider si vous souhaitez prendre un risque plus élevé et avoir des UTXO plus petits, ou si vous souhaitez utiliser une couche 2 ou un dépositaire.

- Il existe 2 façons d'éviter d'avoir de petits UTXO : la première consiste à retirer de plus grandes quantités de bitcoin d'un échange après l'avoir acheté. Par exemple, au lieu d'acheter 50 $ chaque jour et de le retirer quotidiennement dans votre portefeuille, vous pourriez acheter 350 $ une fois par semaine et les retirer une fois par semaine. Ou vous pouvez acheter 50 $ tous les jours et retirer seulement une fois par semaine après avoir échangé 350 $. Vous auriez donc 1 UTXO d'une valeur de 350 $ créé chaque semaine, au lieu d'avoir 7 UTXO d'une valeur de 50 $ chacun créés chaque semaine.

- La deuxième façon d'éviter les petits UTXO est de les consolider. Vous pouvez effectuer une transaction à partir de votre portefeuille qui est soit renvoyée vers le même portefeuille, soit vers un autre portefeuille que vous possédez. Cela vous permettra de recevoir un seul UTXO ayant la valeur de tous vos anciens UTXO combinés, moins les frais de réseau.

- Vous irez sur la page de réception de votre portefeuille et copierez votre propre adresse Bitcoin, puis accéderez à la page d'envoi et collerez votre propre adresse dans l'adresse de destination. Si vous consolidez de nombreux petits UTXO, les frais seront probablement assez élevés, mais il y a de fortes chances que les frais le soient beaucoup plus à l'avenir. C'est donc une bonne idée de consolider chaque fois que vous pensez que les frais sont relativement faibles.

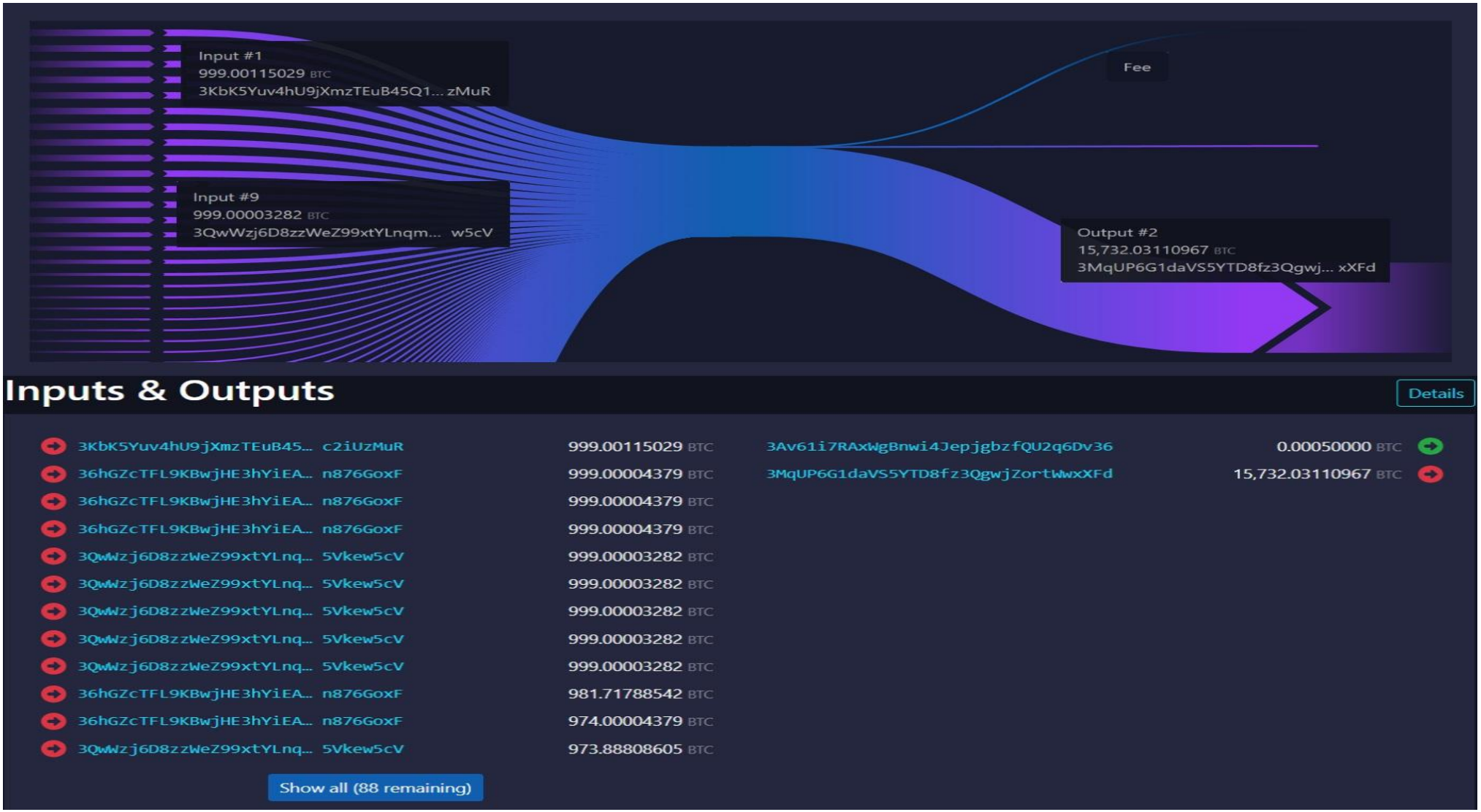



- Ci-dessus se trouve un autre organigramme de mempool.space, il montre une transaction de consolidation. Il y a 5 entrées, chacune d'une taille d'environ 400 000 satoshis, et 2 sorties, d'abord les frais pour les mineurs, puis le nouvel UTXO qui vaut la valeur combinée des 5 entrées, moins les frais bien sûr.

- Même si nous ne savons pas à 100 % que cette transaction est une consolidation par auto-transfert, c'est très probable. Quelqu'un a probablement acheté des morceaux de Bitcoin de 200 $ et les a retirés dans son portefeuille. Il a ensuite décidé de regrouper ces UTXO en un seul gros, en le renvoyant soit dans le même portefeuille, soit dans un autre qu'il contrôle.

- Cette personne possède désormais un satoshi UTXO de près de 2 millions, qu'il sera probablement économiquement viable de dépenser pendant très longtemps, voire pour toujours.

- ***Si vous souhaitez voir une démonstration vidéo de la consolidation UTXO cliquez sur ce lien: [*"UTXO Consolidation"*]***




- Il s'agit d'une transaction intéressante à examiner, elle provient de Grayscale, un émetteur d'ETF. Il va à Coinbase qui est une bourse, et également le dépositaire de certains autres ETF.
- Il y avait 100 entrées et 3 sorties. Chaque entrée était un UTXO détenu par Grayscale, puis consolidé en un UTXO de 15 732 BTC que Coinbase détenait ensuite.
- Étrangement, un UTXO de 50 000 satoshi est également créé. Cela pourrait être la monnaie de change par rapport à la transaction, mais il s'agit d'un très petit montant.


- Ceci est un exemple de transaction par lots ou de transaction à sorties multiples. Il y a un seul UTXO comme entrée et 3 sorties plus la sortie payante. Cette personne peut payer 2 ou 3 portefeuilles, il est difficile de savoir s'il y a une sortie de change qui retourne à l'expéditeur ou si chaque sortie est un nouveau portefeuille. Parfois, la monnaie sera renvoyée à l'adresse qui l'a envoyée, mais de nombreux portefeuilles utilisent une nouvelle adresse.

- En regroupant ces transactions, l'expéditeur économisait sur les frais, car il ne disposait que d'une seule entrée pour payer plusieurs personnes, au lieu d'envoyer des transactions distinctes, ce qui nécessiterait plusieurs entrées et coûterait donc plus cher.

# Frais

- Les frais changent constamment, en fonction de la demande d'espace de bloc.
- Environ 5 000 transactions peuvent être placées dans chaque bloc, donc si vous voulez être dans le bloc suivant, vous devez enchérir pour celui-ci. Imaginez une vente aux enchères dans laquelle quelqu'un vend un terrain de 5 000 hectares en tranches d'un hectare. S'il n'y a que 4 000 personnes souhaitant acheter 1 hectare chacune, le prix baissera et sera relativement bon marché. Mais si 6 000 personnes veulent acheter 1 hectare chacune, une guerre d'enchères peut éclater et le prix pourrait augmenter considérablement.
- Si vous souhaitez attendre plus longtemps et n'avez pas besoin que votre transaction soit incluse dans le bloc suivant, vous pouvez potentiellement payer des frais inférieurs. Bien que cela ne garantisse pas que votre transaction soit bloquée, si trop de personnes continuent de vouloir effectuer des transactions et sont prêtes à payer plus que vous, vous risquez de ne jamais être inclus dans un bloc.
- C'est une bonne idée de visiter un site comme mempool.space pour connaître les frais moyens actuels lors d'une transaction. Si vous choisissez des frais bien inférieurs aux frais moyens actuels, votre transaction pourrait être supprimée du pool de mémoire et renvoyée dans votre portefeuille.
- Le pool de mémoire (mempool) est comme une salle d'attente pour les transactions, où vous allez placer votre offre pour un espace de bloc. Jusqu'à ce qu'un mineur choisisse votre transaction, vous devez attendre dans le pool de mémoire avec une transaction non confirmée.
- Une fois que vous recevez une confirmation que votre transaction a été bloquée, elle est alors considérée comme réglée. Plus une transaction a de confirmations de blocs, plus elle est sécurisée et ne peut pas être annulée par un attaquant du réseau (très improbable).
- Il existe des fonctionnalités appelées RBF (remplacement par frais) et CPFP (enfant paie pour le parent) qui vous permettent d'augmenter les frais d'une transaction au cas où elle ne serait pas exploitée et resterait bloquée dans le pool de mémoire. Voici un lien vers une bonne vidéo qui explique comment les utiliser: "Fixing Stuck Bitcoin Transaction"

# Autres couches

- Le réseau Bitcoin est généralement appelé L1, couche 1 ou couche de base.
- Il existe ensuite des couches supérieures, qui sont différents réseaux au-dessus de la couche de base Bitcoin. Tels que le réseau Lightning, le réseau Liquid, le rootstock, la couche mercury, etc. Il existe de nombreuses couches alternatives, chacune avec des compromis de sécurité variés.
- La deuxième couche la plus fiable et la plus sécurisée créée jusqu'à présent est le réseau Lightning. Il propose des paiements instantanés, sans avoir à attendre des temps de blocage de 10 minutes. Il vous permet également d'effectuer des transactions beaucoup moins chères, en transformant 2 transactions de couche de base, un canal ouvert et un canal fermé, en potentiellement beaucoup plus de transactions hors chaîne, peut-être même des milliers. Le réseau Lightning est un réseau de routage avec des nœuds. C'est comme un modèle en étoile, dans lequel il existe des hubs de routage avec de nombreuses connexions vers les utilisateurs et d'autres hubs.
- C'est comme ouvrir une note de bar, au lieu de glisser votre carte pour chaque boisson, vous n'en faites qu'un seul à la fin de la soirée pour régler la note.
- Vous devez utiliser un nouveau portefeuille pour utiliser le réseau Lightning. Et ayez une autre phrase de récupération secrète à stocker. À moins que vous n'utilisiez Electrum, ou Green de Blockstream, car ces deux éléments ont un wallet Lightning intégré dans leurs portefeuilles de couche 1.
- Vous ne pouvez envoyer et recevoir que certains montants via Lightning, en fonction de vos liquidités entrantes et sortantes. À moins que vous n'utilisiez un portefeuille Lightning de garde, dans lequel vous ne contrôlez pas les clés, vous n'avez pas à vous soucier de la liquidité.
- Plus la quantité de bitcoins que vous envoyez lorsque vous ouvrez un canal Lightning pour la première fois est importante, plus vous pouvez en envoyer et en recevoir. Vous pouvez augmenter votre liquidité, votre solde d'envoi et de réception, en effectuant une autre transaction de niveau 1.

- Lightning aide certes à faire évoluer Bitcoin un peu, mais en fin de compte, il nécessite toujours plusieurs transactions de couche 1 chaque année. Et la couche 1 du Bitcoin est limitée à environ 260 millions de transactions par an. Ainsi, environ 100 millions de personnes peuvent effectuer 2 à 3 transactions par an. Ce qui pourrait être une ouverture et une fermeture de canal Lightning. Nous aborderons la question de la mise à l'échelle plus en détail plus tard dans le cours.

- Le réseau Liquid et rootstock sont des couches semi-conservatrices, avec leurs propres blockchains. Ils ne sont pas aussi sécurisés que la couche de base Bitcoin, car il existe un groupe de personnes qui pourraient potentiellement se réunir pour prendre votre argent ou contrôler la façon dont vous pouvez dépenser. Semblable à une banque ou à une bourse, sauf qu'il est plus transparent et également plus résistant au vol en raison de la nécessité d'un groupe d'individus distincts pour signer les transactions d'un multisig.

- Liquid et rootstock ont plus de fonctionnalités que la couche 1, ils peuvent avoir des actifs alternatifs, effectuer des transactions plus rapides et avoir des choses comme des transactions confidentielles qui sont privées, contrairement à la couche 1. Mais en fin de compte, ils ne sont pas aussi décentralisés ou sécurisés que la couche de base Bitcoin.

- Une autre couche supérieure de Bitcoin est appelée e-cash. Fedimint et Cashu sont des exemples e-cash qui utilisent un système de fédération.

- La fédération peut créer une monnaie distincte liée au prix du bitcoin et bloquer le bitcoin en échange de la nouvelle monnaie. De la même manière que fonctionnait l'étalon-or, une banque donnerait aux gens des billets de banque en échange d'une quantité spécifique d'or, et si l'utilisateur de la banque souhaite récupérer son or, la banque promettrait d'échanger les billets de banque contre de l'or.

- Ce système e-cash peut être très privé, mais un groupe de personnes pourrait néanmoins se coordonner pour vous voler, même s'ils devraient voler tout le monde en même temps dans un système e-cash privé.

- Ces transactions en e-cash sont hors chaîne, elles peuvent donc faire évoluer les paiements Bitcoin et permettre davantage de transactions sans avoir à payer de frais de couche 1.

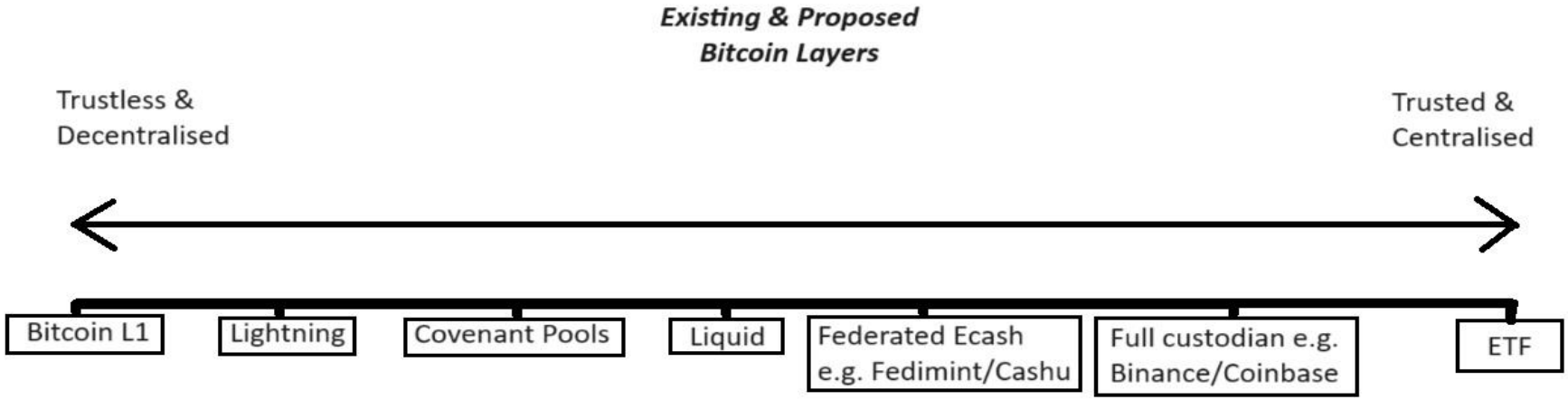
- Vous pourriez avoir une fédération familiale ou communautaire locale. Ceci est parfois appelé le modèle Oncle Jim, dans lequel un membre de la famille connaissant le bitcoin, Oncle Jim, conserve le bitcoin et émet un jeton en espèces contre le bitcoin qui est verrouillé. Avec le jeton e-cash, les gens pourraient effectuer des transactions à très bas prix, voire gratuitement, avec toute personne disposée à accepter l'e-cash d'Oncle Jim.

- Une autre couche de bitcoin, qui, selon certains, ne devrait pas du tout être considérée comme une couche de bitcoin en raison de l'absence de garantie que vous pouvez retirer, celle des dépositaires à part entière. Il s'agit d'échanges, d'ETF, de banques, etc. dont vous ne détenez pas les clés. Les dépositaires permettent une interface utilisateur plus simple et peuvent rendre les transactions moins chères et permettre des choses comme la récupération de fonds avec l'aide d'une personne de l'entreprise. Mais le dépositaire contrôle votre bitcoin et pourrait facilement vous voler ou limiter la façon dont vous pouvez dépenser votre bitcoin.

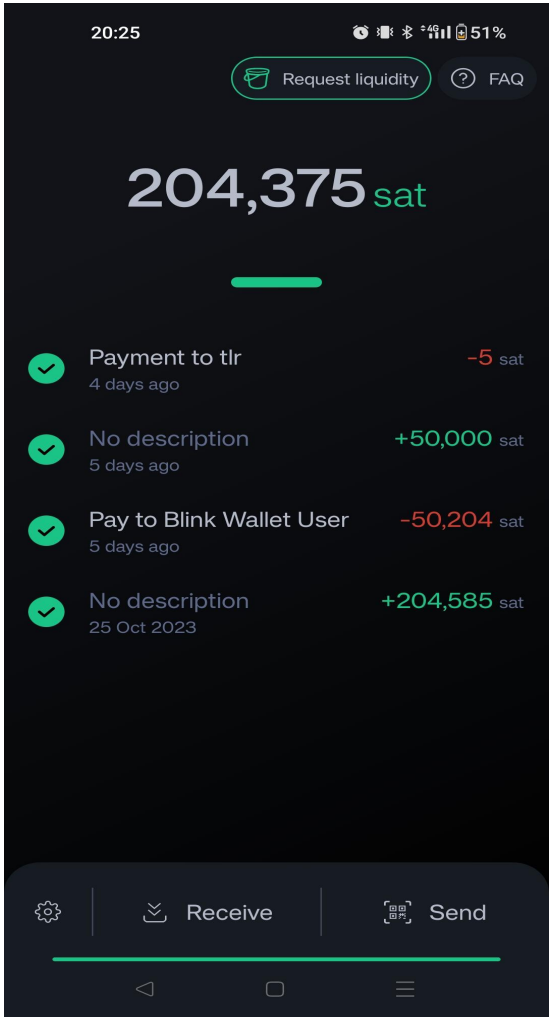
- La dernière solution de mise à l'échelle dont je parlerai concerne les clauses restrictives. Ceux-ci n'existent pas vraiment actuellement dans Bitcoin, mais ils sont en cours de discussion et pourraient constituer une future mise à niveau potentielle du système. Les covenants sont des contrats auxquels vous vous portez volontaire et qui peuvent limiter l'endroit où votre portefeuille peut envoyer des bitcoins. Cela signifie que vous pouvez conclure un contrat prouvant que vous paierez quelqu'un à l'avenir et que vous ne pouvez pas l'annuler.

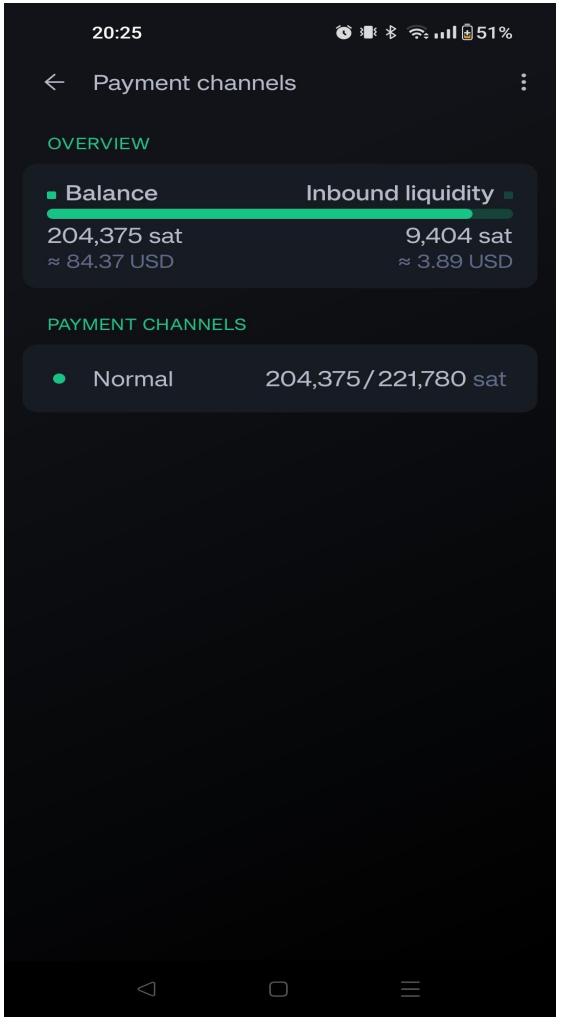
- Un type d'engagement qui existe dans Bitcoin est le verrouillage temporel. Où vous pouvez choisir de verrouiller votre bitcoin dans un portefeuille pendant une durée prédéterminée. Cette utilisation est 100 % volontaire pour l'utilisateur.

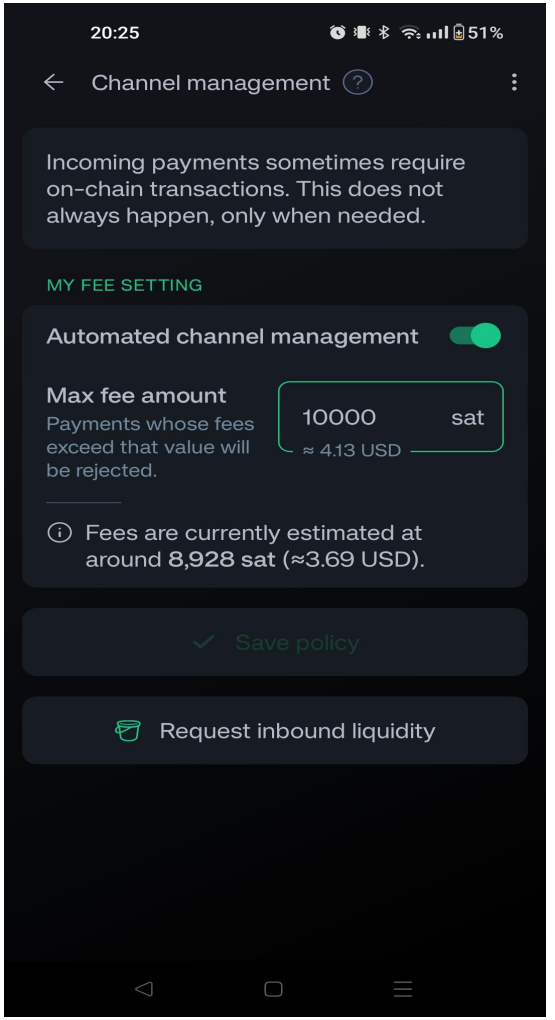
- Les contrats prouvables permettent aux utilisateurs de partager un seul UTXO, compressant essentiellement les transactions. Les clauses restrictives sont très complexes. Ce qui compte, c'est qu'elles contribuent à faire évoluer le bitcoin et à améliorer la confidentialité et l'auto-garde. Tout en étant également un changement très conservateur et mineur, avec un faible risque de problèmes futurs.




- Le graphique ci-dessus montre à quel point chacune des couches dont nous venons de parler est décentralisée et sans confiance. Plus la couche est éloignée de L1, moins vous devez y conserver d'argent.
- L'image de droite est le pool de mémoire du réseau Liquid. Comme vous pouvez le voir, les blocs sont toutes les 1 minutes au lieu de 10 comme sur L1.
- Il n'a pas non plus beaucoup d'utilisateurs et les blocs sont très vides.




- Il s'agit du portefeuille Lightning Phoenix. C'est l'un des portefeuilles Lightning les plus populaires et les plus fonctionnels. Il est autonome et open source, vous devrez stocker une nouvelle phrase de départ.

- La première image est la page d'accueil, vous pouvez voir un exemple de portefeuille, avec un historique des transactions. La deuxième image vous montre chaque canal que vous avez ouvert et le montant de vos liquidités. Ce portefeuille n'a qu'un seul canal, d'une capacité totale d'environ 215 000 satoshis. La barre verte montre comment la liquidité entrante change à mesure que vous dépensez des satoshis depuis le canal. Donc, pour recevoir du Bitcoin, vous devez d'abord en dépenser. Ce n'est pas idéal, mais c'est ainsi que fonctionne actuellement Lightning. La troisième image montre la page de gestion des canaux où vous contrôlez les frais.

# Privacy

- Bitcoin est une blockchain publique, où vous pouvez retracer l'historique des transactions.
- Il s'agit d'un système pseudonyme, ce qui signifie que les gens ne connaissent pas votre vrai nom, votre adresse ou votre identité, mais ils pourraient potentiellement le découvrir en fonction de la personne avec qui vous effectuez une transaction. Par exemple, si vous avez un compte d'échange, comme Binance ou Coinbase, enregistré avec votre nom et votre adresse, alors si vous envoyez de Binance vers votre portefeuille matériel, il est prudent de supposer que Binance et le gouvernement savent que vous contrôlez le portefeuille qui a reçu le bitcoin.
- Si vous souhaitez rester privé et ne pas permettre à tous ceux qui vous envoient de l'argent de voir l'historique et le solde de vos transactions, vous ne devez jamais réutiliser une adresse de réception ou une clé publique. Chaque adresse a une histoire distincte. La plupart des portefeuilles vous donneront automatiquement une nouvelle adresse de réception chaque fois que vous en demanderez une.
- Si vous avez besoin d'une adresse fixe pour recevoir des paiements, il existe d'autres moyens de le faire et de rester privé. Comme le serveur BTCPay en utilisant une couche différente telle que Lightning hors chaîne.
- KYC signifie Connaissez votre client. C'est à ce moment-là que vous devez effectuer une vérification d'identité sur les échanges, les services ou les applications. Par exemple, leur indiquer votre e-mail, votre numéro de téléphone, votre nom, votre adresse et télécharger votre passeport/pièce d'identité.
- Ces données KYC pourraient être utilisées par le gouvernement pour vous taxer ou vous punir. Ou bien il pourrait potentiellement être divulgué, ce qui entraînerait une attaque ou une arnaque à votre égard. Il peut également être utilisé par le gouvernement pour vous suivre et potentiellement contrôler la façon dont vous utilisez votre bitcoin.

- Vous pouvez également obtenir certains types de confidentialité à partir d’autres couches de Bitcoin. Lorsque vous utilisez le réseau Lightning, les transactions s'effectuent hors chaîne et ne font pas partie d'un grand livre public. Les seules personnes qui peuvent voir vos transactions sont les personnes à qui vous les envoyez et les nœuds Lightning qui aident à acheminer votre paiement.

- Le réseau Liquid est une autre couche qui offre une confidentialité supplémentaire, en utilisant des transactions confidentielles. Ceux-ci permettent à l'expéditeur de garder le montant de la transaction privé ainsi que l'actif de la transaction, car Liquid peut avoir d'autres actifs que Bitcoin.

- OpSec (Operational Security) ou la sécurité opérationnelle en français est votre image publique en ce qui concerne votre richesse Bitcoin et la façon dont vous la stockez. Vous devez vous limiter au minimum à savoir qui sait que vous possédez du Bitcoin et combien vous en possédez.

- Éviter les liens KYC est toujours la meilleure solution, afin d'éviter que les sociétés de surveillance ou les gouvernements tentent de vous suivre et de vous juger en fonction de l'historique de vos transactions. Ou pour essayer de vous voler. Il est préférable qu'ils croient que vous n'avez rien, ou du moins qu’on ne puisse pas prouver que vous possédez des bitcoins.

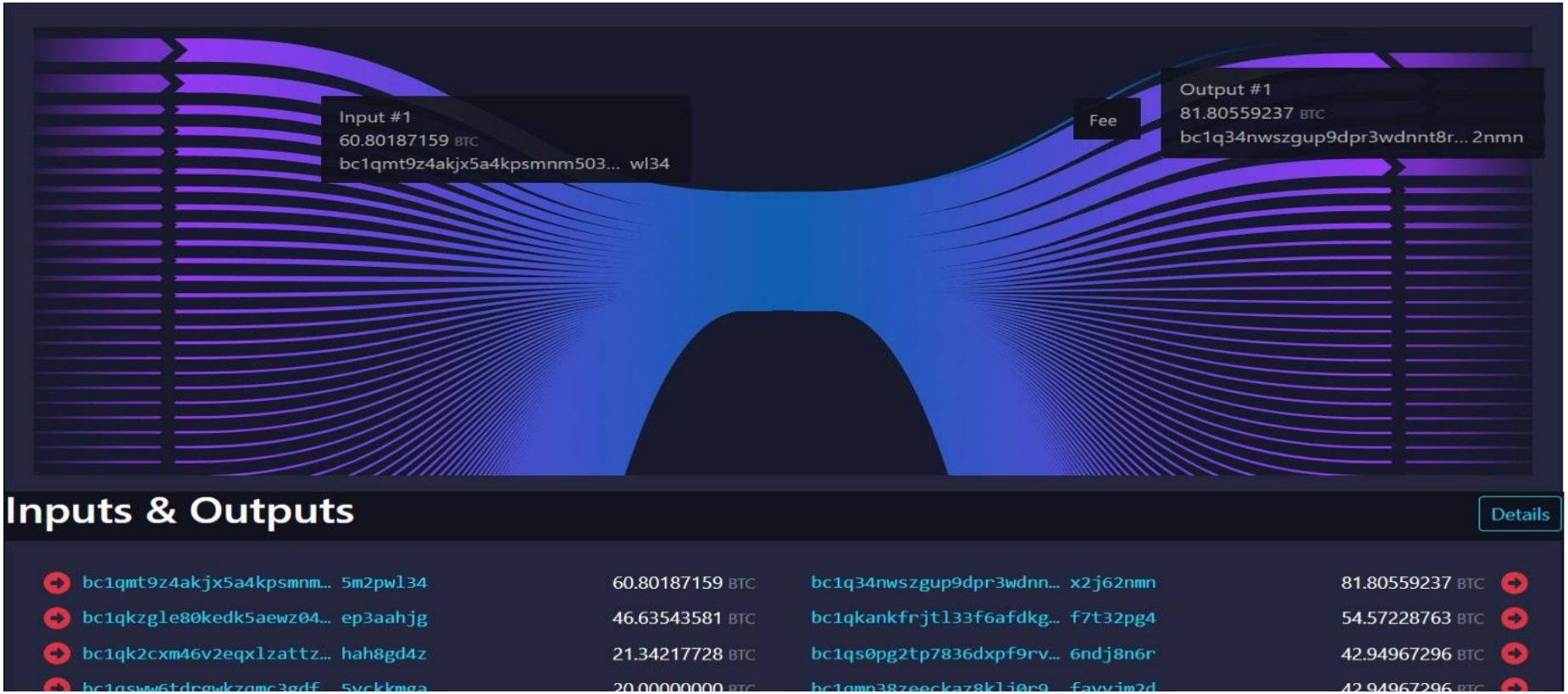
- Vous pouvez bien sûr toujours prétendre que vous avez perdu vos clés et que vous ne pouvez plus accéder à votre bitcoin. Il existe des moyens de rendre cela plus crédible, par exemple en transférant votre bitcoin plusieurs fois avant de le stocker dans votre portefeuille. Il y a un mème dans Bitcoin selon lequel de nombreuses personnes ont perdu leurs clés dans un accident de bateau.

- Lorsque vous discutez de Bitcoin en ligne, il est préférable de le faire de manière anonyme si possible. En fin de compte, il s’agit d'éviter que les gens tentent de vous arnaquer et d'éviter que les gens ne tentent de vous extorquer, peut-être avec violence. Il existe de nombreuses histoires de personnes torturées jusqu’à ce qu’elles abandonnent leur bitcoin. Bien entendu, cela pourrait se produire avec ou sans Bitcoin. La principale différence est que, à moins que vous n’ayez pris des covenants, une fois qu’ils ont volé votre bitcoin, personne ne peut faire grand-chose pour le récupérer pour vous. Contrairement à une banque, où l’argent peut être gelé ou annulé. Mais cela fait partie de la responsabilité qui accompagne la possibilité de ne pas avoir besoin de faire confiance à quelqu’un pour stocker votre argent.

# CoinJoin

- Il existe des moyens de briser la chaîne de l'historique des transactions. Vous pouvez utiliser un service coinjoin. Cela regroupe les transactions de nombreuses personnes dans une seule transaction par lots, puis la divise à nouveau plus tard, ce qui rend impossible de savoir quel historique de transaction appartient à quelle adresse qui a reçu les bitcoins. Plus il y a de personnes à l'intérieur du coinjoin, plus votre vie privée est grande.

- Vous trouverez ci-dessous un autre diagramme de flux de mémoire qui montre une coinjoin se produisant sur la blockchain. De nombreuses entrées sont entrées dans une transaction et un nombre égal de sorties sont créées, récompensant tous ceux qui sont entrés dans la coinjoin avec de nouveaux satoshis et de nouveaux UTXO qui ne peuvent pas être retracés avant la coinjoin.



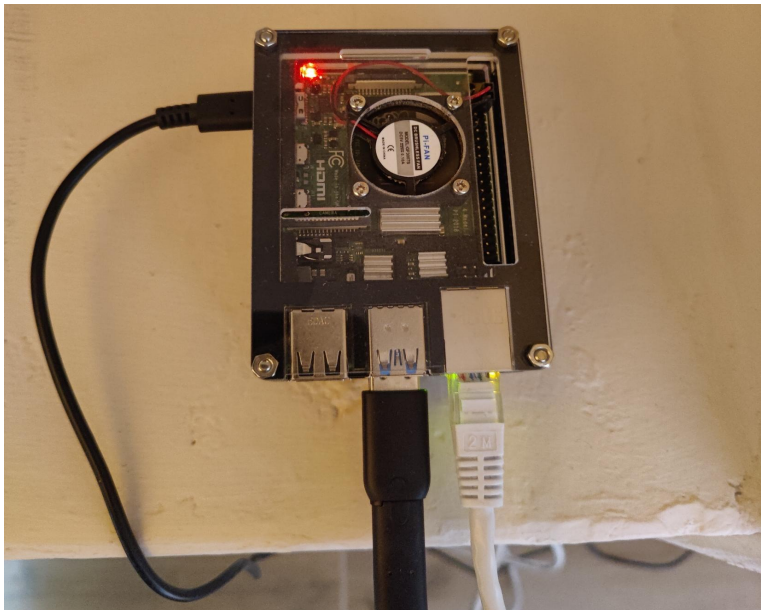
# Nœuds

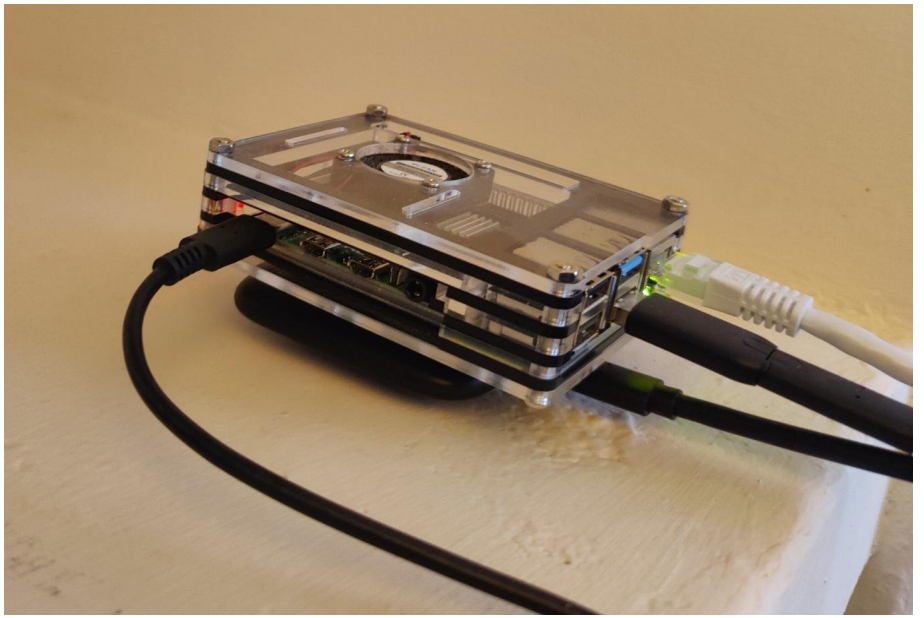
- Un nœud est un ordinateur qui exécute le logiciel Bitcoin et applique les règles du réseau. Chaque copie du logiciel peut décider des règles qu'elle souhaite appliquer, mais si vous essayez d'appliquer une règle qui rompt le consensus, vos transactions seront invalides et ne seront pas minées dans un bloc.

- Le nœud contient également un historique de la blockchain, toutes les transactions qui ont été minées dans des blocs dans le passé. Actuellement, cela représente environ 600 Go de données.

- Vous pouvez connecter un portefeuille à votre nœud afin de vérifier que les transactions que vous effectuez sont réellement incluses dans la blockchain et que vous possédez réellement les pièces que votre portefeuille indique posséder. Si vous n'exécutez pas de nœud, cela signifie que vous faites confiance au nœud de quelqu'un d'autre pour vous donner la vérité, les incitations du système font en sorte qu'il y a très peu de chances qu'on vous mente. Cependant, si vous souhaitez être véritablement souverain à 100 % sur Bitcoin, vous devez exécuter votre propre nœud.

- Ci-dessous quelques photos de mon nœud, qui est installé sur un Raspberry Pi.





- Plus votre nœud vérifie de transactions réelles, plus son pouvoir économique ou son poids dans le système est grand. Cela signifie que les règles du réseau sont davantage influencées par la configuration de vos nœuds que par le nœud de quelqu'un qui ne vérifie pas grand-chose.

- Si un gouvernement voulait reprendre le contrôle de Bitcoin et apporter des modifications au code, il devrait empêcher les utilisateurs de Bitcoin d'exécuter un nœud. Ce qui est extrêmement difficile car un nœud Bitcoin peut se trouver sur presque n'importe quel type d'ordinateur et il s'agit d'un logiciel qui peut être facilement masqué et déplacé. Et ils devraient faire plus que simplement exécuter leurs propres nœuds, car comme mentionné ci-dessus, un nœud a plus d'influence sur les règles du réseau s'il vérifie de nombreuses transactions de première main.

- Un exemple de nœud économique manifestement puissant est une bourse, comme Binance. Ils vérifient directement de nombreuses transactions au nom de leurs utilisateurs.

- Alors, comment obtenir un nœud ? Achetez soit un Raspberry Pi, un ordinateur portable bon marché ou un ordinateur de bureau bon marché, avec un disque dur de 2 To et plus de 4 Go de RAM. Certaines entreprises vendent également des nœuds préconstruits que vous pouvez simplement brancher, mais ils sont plus chers. Vous avez alors besoin d'un système d'exploitation, Linux est le mieux adapté pour un nœud Bitcoin, mais cela peut également se faire sur Windows ou Apple. Ensuite, vous téléchargez Bitcoin Core et synchronisez votre nœud avec le réseau, en effectuant le téléchargement en bloc initial, qui peut prendre des heures ou des jours, en fonction de votre matériel et de la vitesse d'Internet.

- Vous pouvez également télécharger une suite logicielle, telle que Umbrel ou Start9, qui disposent de leur propre système d'exploitation et de leurs propres magasins d'applications. Vous l'installez directement sur un ordinateur avec une carte USB ou SD. Ceux-ci sont plus simples à configurer et sont également livrés avec de nombreuses autres applications intéressantes pour vous aider avec un serveur domestique, des outils de confidentialité et d'autres applications de service Bitcoin comme un nœud Lightning. Cependant, vous êtes légèrement moins souverain car vous faites confiance au code d'un tiers et vous ne pouvez mettre à jour le noyau Bitcoin que lorsqu'il vous donne la mise à jour, il peut également modifier la mise à jour. Ce n'est pas un gros problème car ils se sont montrés très justes et rapides avec les mises à jour, mais c'est une possibilité.

# Forks

- Un fork est une modification des règles du consensus Bitcoin, via une modification du code. Il peut s'agir d'un soft fork ou d'un hard fork.
- Un soft fork est une modification des règles de consensus qui est toujours rétrocompatible. Cela signifie que si vous ne mettez pas à jour le logiciel de votre nœud, vous pouvez toujours utiliser le réseau et créer des transactions valides. Afin d'être sûr et sécurisé, vous avez besoin que la majorité économique des nœuds prennent en charge le soft fork et mettent à jour leurs nœuds pour inclure les nouvelles règles.
- Si vous voulez avoir votre mot à dire sur la question de savoir si un soft fork se produit, vous devez disposer d'un nœud qui vérifie les transactions.
- Un hard fork est une modification des règles de consensus qui n'est pas rétrocompatible. Cela signifie qu'une nouvelle blockchain sera créée et toute personne qui ne mettra pas à niveau son nœud sera sur un réseau différent de celui des personnes qui auront mis à niveau le leur. Cependant, si le nouveau réseau avec les nouvelles règles ne dispose pas d'une majorité de nœuds économiquement puissants qui le soutiennent, alors ils seront sur la blockchain minoritaire et il ne sera pas considéré comme du vrai bitcoin.
- Il y a eu de nombreux hard forks dans l'histoire du bitcoin, conduisant à de nouvelles monnaies en raison d'un soutien minoritaire. Quelques exemples de ces forks sont Bitcoin Cash, Bitcoin SV et Bitcoin Gold. Tous ces forks valent bien moins que le Bitcoin. Lorsque ces forks ont été créés, tous ceux qui détenaient du bitcoin ont reçu un montant égal de la nouvelle monnaie de la blockchain, telle que BCH ou BSV. Vous pouvez alors soit conserver ces deux devises, soit vendre l'une contre l'autre. La plupart des gens ont vendu les nouvelles pièces hard fork contre le véritable bitcoin original.
- Toutes les tentatives de soft fork doivent être minutieusement examinées et contestées, pour savoir si elles contiennent des bugs potentiels ou si elles peuvent affecter négativement le système d'incitation, avant de tenter de les activer sur la chaîne L1 principale.

- Vous trouverez ci-dessous un tableau montrant l'historique des forks depuis 2012. Il y a eu environ 10 forks entre 2009 et 2012, mais ceux-ci étaient très faciles à réaliser, car le bitcoin était très récent et encore au début de son développement.

- Parfois, il faut beaucoup de temps pour activer un nouveau soft fork, ce qui est une caractéristique du bitcoin qui le rend si résilient et résistant à la censure. Cependant, il est important de se rappeler que Bitcoin est toujours en cours de développement et d'amélioration, des changements doivent donc encore être apportés à l'avenir pour nous permettre d'évoluer, d'améliorer la confidentialité et d'améliorer les outils d'auto-garde.

- Tout le monde n'a pas besoin d'avoir une opinion sur les soft forks, seulement ceux qui veulent vraiment comprendre en profondeur et peuvent y consacrer du temps. Tout comme ce n'est probablement pas la meilleure solution que de laisser tout le monde dans un pays voter sur chaque décision économique qu'il ne comprend pas vraiment. Tant que l'opportunité d'apprendre et de s'impliquer est disponible.

- L'une des principales leçons de la communauté Bitcoin est de ne pas faire confiance, mais de vérifier. Cela signifie que vous ne devriez pas simplement faire confiance à la parole des autres, mais plutôt faire le travail vous-même en effectuant des recherches ou en examinant le code si vous en êtes capable.

| Time Since Last Fork: | Date: | Fork: |
|---|---|---|
| 18 Months | Mar, 2012 | BIP30 |
| 1 Month | Apr, 2012 | BIP16 |
| 11 Months | Mar, 2013 | BIP34 |
| 28 Months | Jul, 2015 | BIP66 |
| 5 Months | Dec, 2015 | BIP65 |
| 7 Months | Jul, 2016 | BIP68-112-113 |
| 13 Months | Aug, 2017 | BIP141-143-147 (Segwit) |
| 51 Months | Nov, 2021 | BIP341 (Taproot) |

# Limites, problèmes et risques

- Malheureusement, Bitcoin n'est pas parfait. Maintenant que vous comprenez la plupart des aspects du Bitcoin, nous devrions discuter de certains des domaines dans lesquels Bitcoin pourrait s'améliorer et de certains problèmes qui pourraient être capable ou non d'être résolus.

- L'objectif principal du Bitcoin est de séparer l'argent de l'État, de retirer au gouvernement le pouvoir de créer de l'argent. Pour y parvenir, nous avons besoin qu'un nombre important de personnes conservant elles-mêmes leur bitcoin, et ne se contentent pas de le confier aux dépositaires. Dans l'état actuel du code Bitcoin, il n'est pas clair si nous pouvons dépasser quelques centaines de millions de personnes utilisant le réseau de manière très limitée. Comme nous l'avons mentionné précédemment, Bitcoin peut effectuer environ 260 millions de transactions par an sur la couche de base. Ainsi, environ 100 millions de personnes peuvent ouvrir et fermer un canal Lightning chaque année, ce qui, en réalité, n'est pas suffisant. C'est l'une des raisons pour lesquelles nous devons apporter davantage de soft forks avant que le réseau ne s'ossifie et ne devienne incapable de changer en raison de sa taille. On estime qu'environ 20 % des personnes utilisant l'auto-garde suffiront à garder les gardiens sous contrôle.

- Si trop de personnes transfèrent leurs bitcoins chez un dépositaire, comme un ETF ou une bourse, nous pourrions avoir une répétition de l'étalon-or. Où finalement les banques et les gouvernements créent des reconnaissances de dette et gonflent l'offre, finissant par décorréler l'actif monétaire sain sous-jacent. Si vous détenez des bitcoins auprès d'un dépositaire, vous êtes également vulnérable à la censure car vous ne contrôlez pas votre propre argent.

- La centralisation du minage constitue un autre risque majeur pour le Bitcoin. Si le pouvoir de hachage minier devient trop concentré entre les mains de quelques entreprises, elles seront très susceptibles d'être capturées par un gouvernement ou une entité hostile. Ils pourraient être payés ou forcés de censurer, d'exploiter des blocs vides ou d'essayer de réorganiser l'historique de la blockchain s'ils ont plus de 50 % de la puissance de hachage sous leur contrôle. Les gens travaillent toujours sur les moyens d'améliorer cette situation et créent de nouveaux outils pour améliorer la décentralisation minière.

- Un autre problème auquel Bitcoin est confronté concerne sa fongibilité. La fongibilité indique à quel point chaque satoshi est égal, pouvant dépenser n'importe quel satoshi dans n'importe quel endroit acceptant le bitcoin. En raison de la nature publique du bitcoin et de la capacité de suivre les transactions, vos satoshis pourraient être corrompus. Par exemple, en raison d'une liste noire du gouvernement, dans laquelle certaines pièces sont considérées comme sales parce qu'elles ont été impliquées dans un certain type de crime.

- Heureusement, comme nous l'avons vu plus tôt, il existe des techniques de confidentialité qui peuvent restaurer la fongibilité du bitcoin concerné. Comme utiliser un coinjoin ou passer à un couche 2.

- Dans sa forme actuelle, le bitcoin est relativement complexe à gérer soi-même, comme vous l'avez peut-être découvert tout au long de ce cours. Bien sûr, être votre propre banque comportera une certaine complexité, mais nous devrions viser moins. De nombreuses personnes ne seront pas capables ou ne voudront pas assumer la responsabilité de leur propre garde. Nous devons donc créer des solutions qui rendent les choses aussi simples que possible et réduisent la possibilité pour les dépositaires d'abuser de leurs clients. Il est inévitable que certaines personnes aient recours à une forme de service de garde. Nous verrons probablement des banques Bitcoin, peut-être simplement une évolution des échanges actuels.

- Le succès du Bitcoin sur le marché libre n'est pas non plus garanti. Il est toujours possible qu'une autre monnaie présente de meilleures propriétés que le Bitcoin et dépasse son adoption. Il ne faut pas trop s'en inquiéter, car cela serait très improductif et ralentirait l'évolution monétaire en cours. Mais il est bon d'être préparé et d'avoir un plan pour l'avenir.

- Un autre problème avec Bitcoin dont je pense que tout le monde devrait être conscient est qu'avant 2140, nous devons faire un hard fork pour corriger un bug qui est bien compris. Lorsque la subvention globale sera épuisée, il y aura un problème avec le logiciel qui l'empêchera de fonctionner. Heureusement, il devrait être facile de convaincre les gens de mettre à niveau leurs nœuds, car s'ils ne le font pas, ils ne seront plus sur une blockchain fonctionnelle. Mais les gens devront faire attention à la version de Bitcoin vers laquelle ils choisissent de mettre à niveau, cela pourrait créer un possibilité de tenter une attaque sur le système. Les incitations financières devraient être telles que personne ne veuille vraiment attaquer le bitcoin.

# Dépenser du bitcoin

- L’un des éléments essentiels de Bitcoin est qu’il incite les gens à épargner davantage et à dépenser moins. Surtout pendant la phase d’adoption où le prix augmente de façon plus spectaculaire et la volatilité est élevée. Mais bien sûr, nous devons quand même en dépenser pour avoir une vie belle et heureuse.

- Dépenser du bitcoin est utile pour faire progresser l’adoption et créer une économie circulaire. Si vous dépensez du bitcoin dans une entreprise, celle-ci est plus susceptible de continuer à l’accepter et à faire connaître le Bitcoin aux autres.

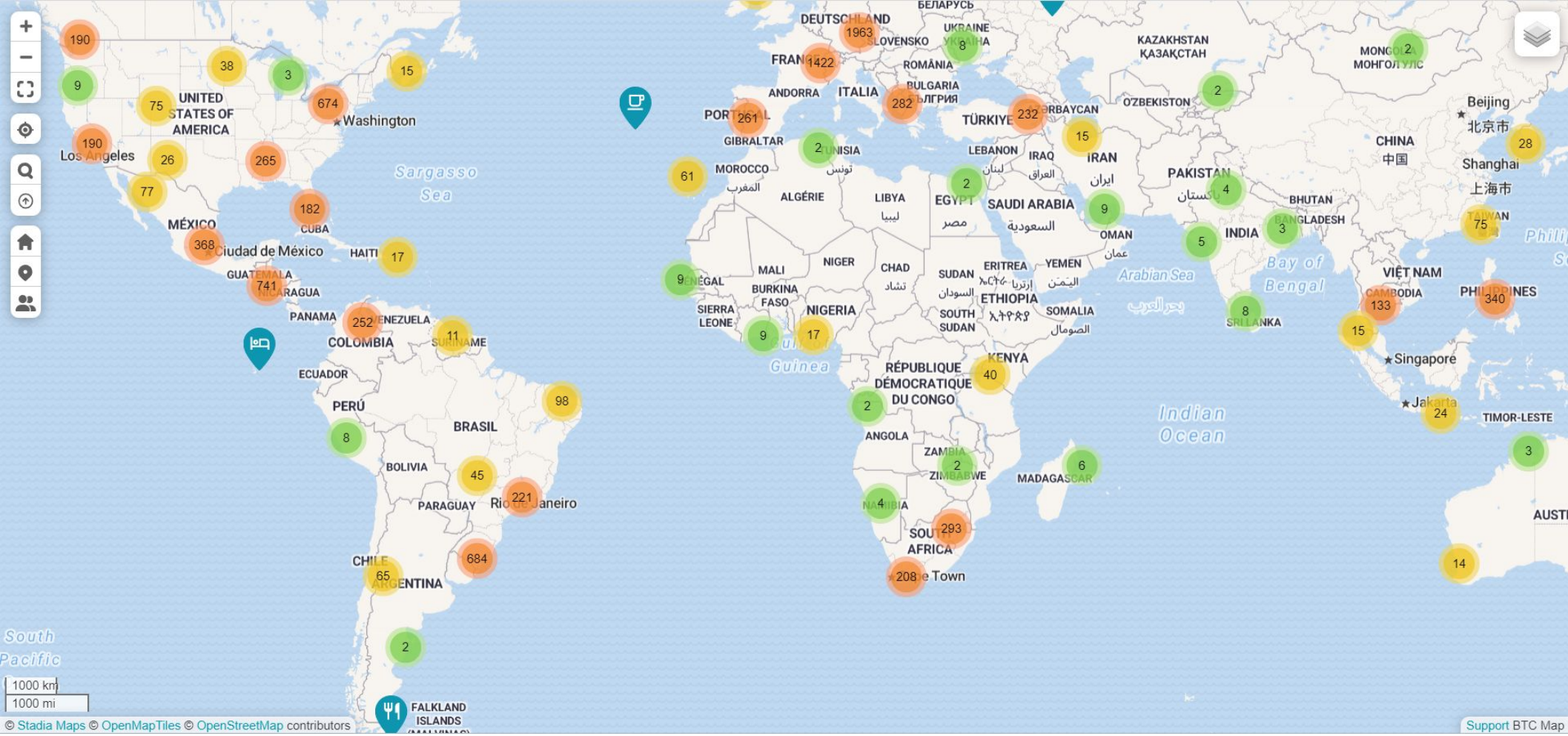
- Cela ne signifie pas que vous devez avoir moins de bitcoins, si vous avez de l'argent fiduciaire que vous auriez dépensé pour quelque chose, mais au lieu de cela, vous avez dépensé du bitcoin, vous pouvez remplacer le bitcoin que vous avez dépensé en en achetant davantage avec votre argent fiduciaire. C'est ce qu'on appelle dépenser et remplacer.

- Chaque année, de plus en plus d'entreprises acceptent le bitcoin comme moyen de paiement, tant en ligne que dans le monde réel. Certains d’entre eux choisiront de vendre le bitcoin qu’ils reçoivent contre de la monnaie fiduciaire, et d’autres choisiront de conserver le bitcoin.

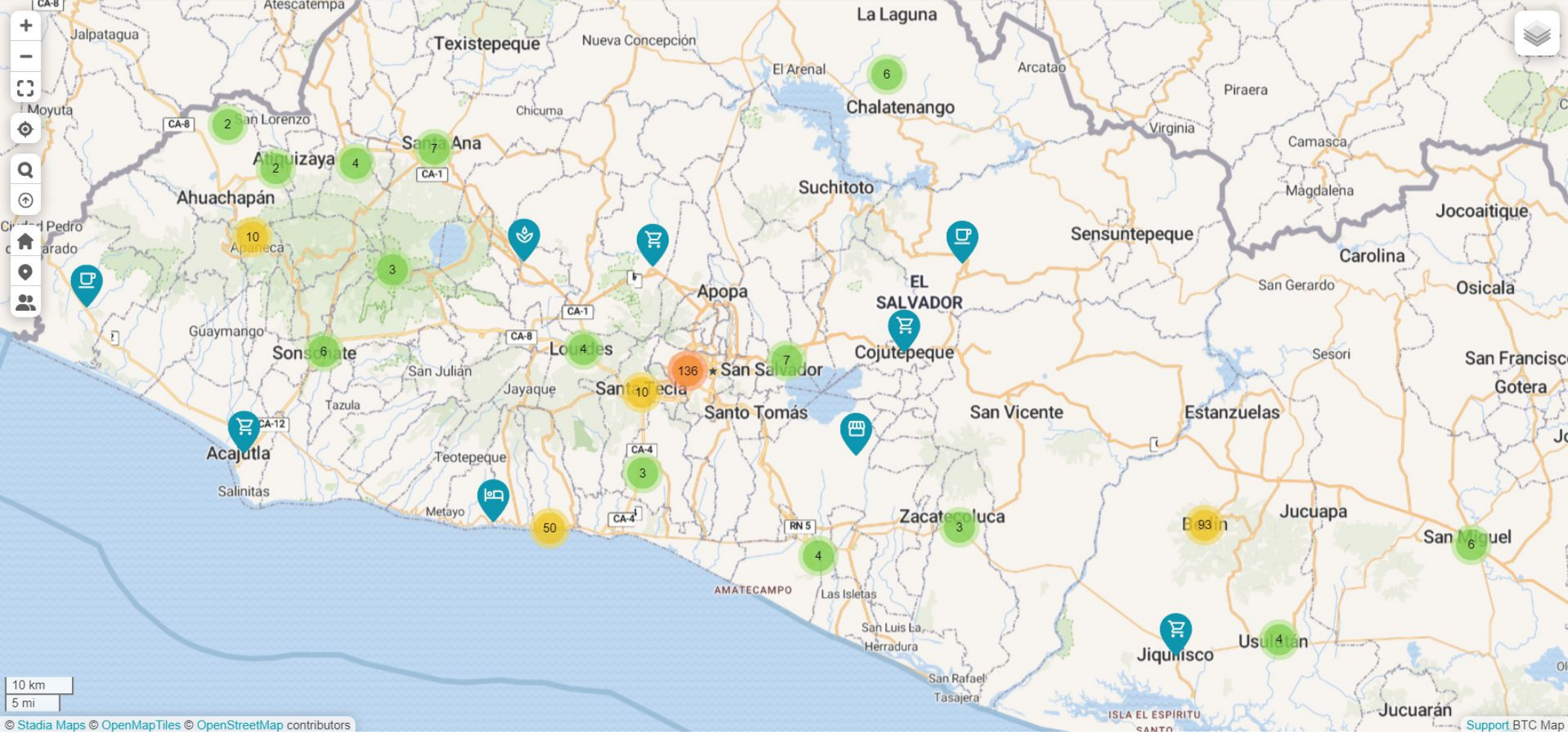
- Il existe de nombreuses entreprises en ligne où vous pouvez également dépenser votre bitcoin. Quelques exemples sont: https://shopinbit.com/ https://shop.lnbits.com/ https://thebitcoincompany.com/ https://www.bitrefill.com/us/en/ https://store.coinkite.com/store

- La meilleure façon de trouver des entreprises qui acceptent le Bitcoin est de rechercher sur https://btcmap.org/. Il s’agit d’une carte du monde sur laquelle sont épinglées la plupart des commerces qui acceptent Bitcoin. C'est un outil très utile lorsque vous êtes en voyage. Nous aborderons cet outil au cours des prochaines diapositives, pour voir où vous pouvez dépenser du BTC.

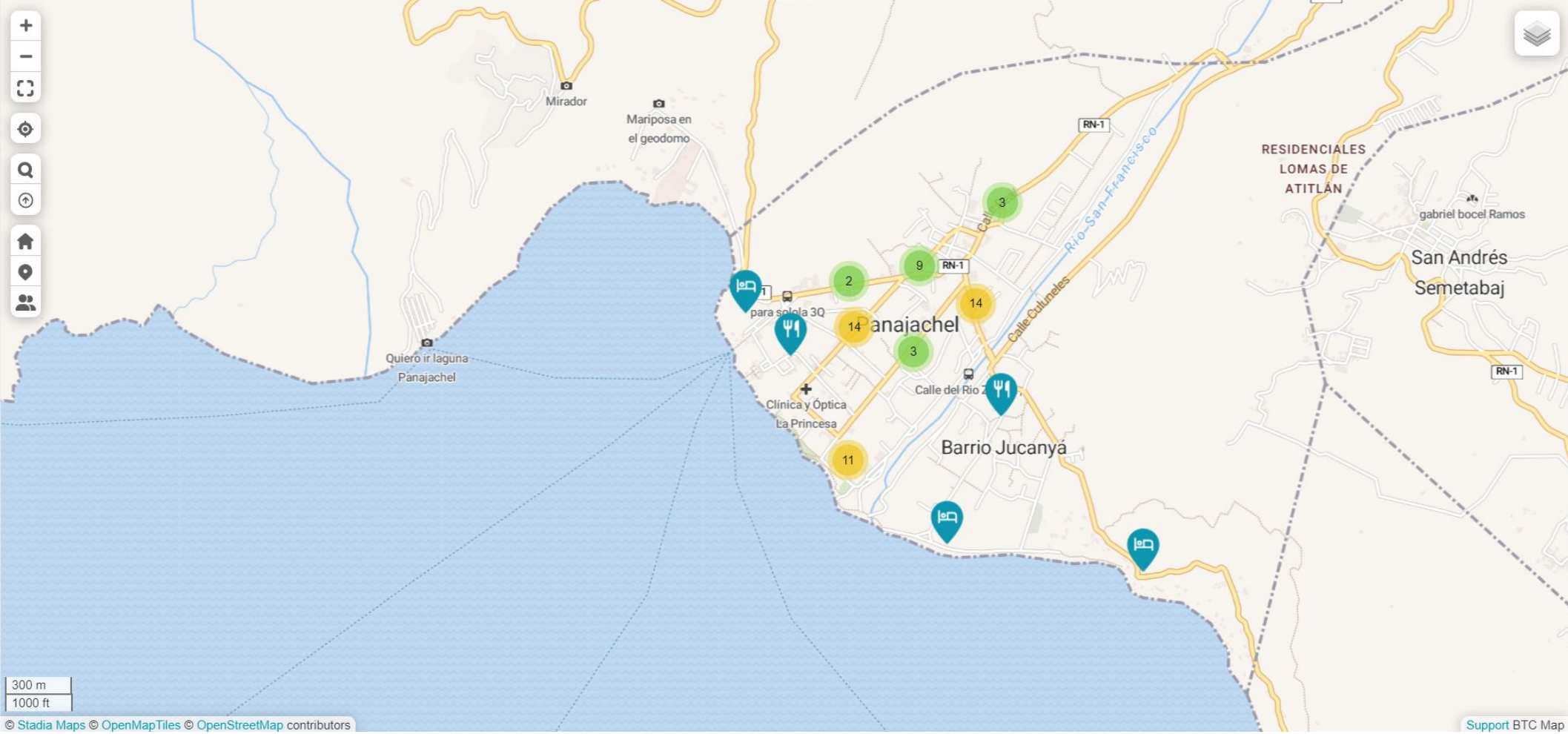
- La plupart du temps, lorsque vous dépensez du bitcoin, vous pourrez utiliser le réseau Lightning, et vous le souhaiterez car il est beaucoup moins cher. C’est une raison pour toujours garder quelques satoshis dans un portefeuille Lightning, et de recharger celui-li lorsque le mempool n’est pas surchargé.




- Ci-dessus se trouve la vision du monde de BTCMap, des milliers d'entreprises acceptent le bitcoin épinglé sur cette carte.
- Actuellement, il n’existe qu’un seul pays où le Bitcoin a cours légal. C'est le Salvador. Vous pouvez dépenser des bitcoins presque partout, du McDonald's au supermarché en passant par un taxi. Le cœur et l’origine de l’économie Bitcoin au Salvador est Bitcoin Beach à El Zonte.
- Nous examinerons de plus près le Salvador et son histoire avec le Bitcoin, ainsi que certaines des autres communautés et hotspots Bitcoin à travers le monde.



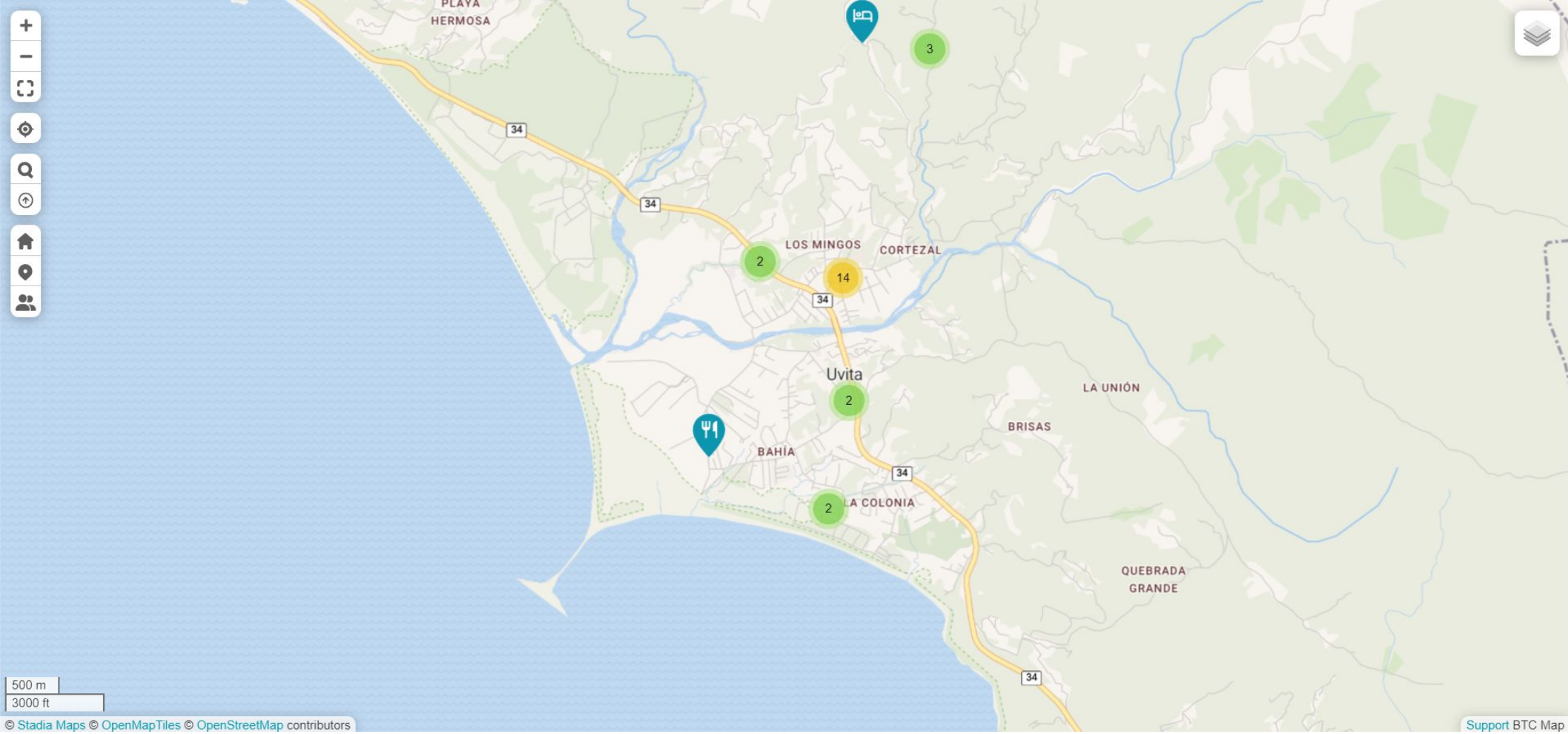

- Il existe 2 zones principales du Salvador avec une forte utilisation du Bitcoin : la capitale San Salvador et la ville d'El Zonte sur la côte, où se trouve le numéro jaune 50.
- Étant donné que le bitcoin a cours légal au Salvador, depuis 2021, il existe en fait beaucoup plus d'endroits qui acceptent le bitcoin que sur cette carte. La plupart des endroits sur cette carte sont des entreprises appartenant à des bitcoiners.
- Le gouvernement salvadorien participe également au minage de bitcoins, en utilisant l'énergie géothermique générée par les nombreux volcans du pays. Ils émettent également des obligations Bitcoin pour acheter davantage de Bitcoin et investir davantage dans l'exploitation minière géothermique, ce qui contribuera à augmenter la production d'énergie dans le pays.



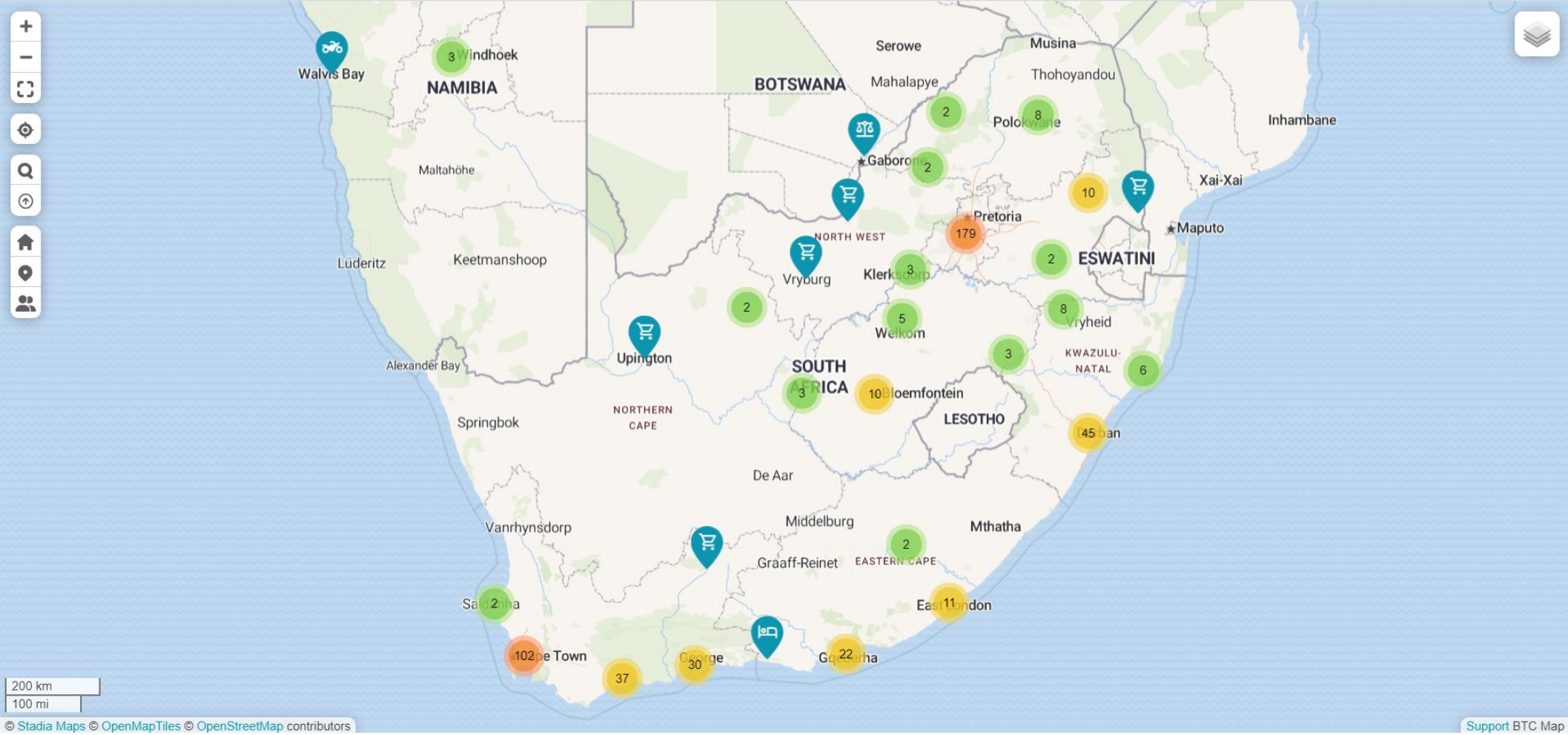

- Juste de l’autre côté de la frontière du Salvador, au Guatemala, l’adoption du Bitcoin augmente également rapidement. Le lac Atitlan a été nommé Bitcoin Lake par de nombreuses personnes qui y vivent, un nom qui s'associe à Bitcoin Beach au Salvador.

- Dans le petit village de Panajachel, au bord du lac, de nombreuses entreprises acceptent le bitcoin, plus de 30 d'entre elles. Et ce n'est pas un grand endroit. Il s’agit d’un excellent exemple d’économie circulaire Bitcoin et de la manière dont elle peut avoir un impact positif sur les zones qui l’entourent.

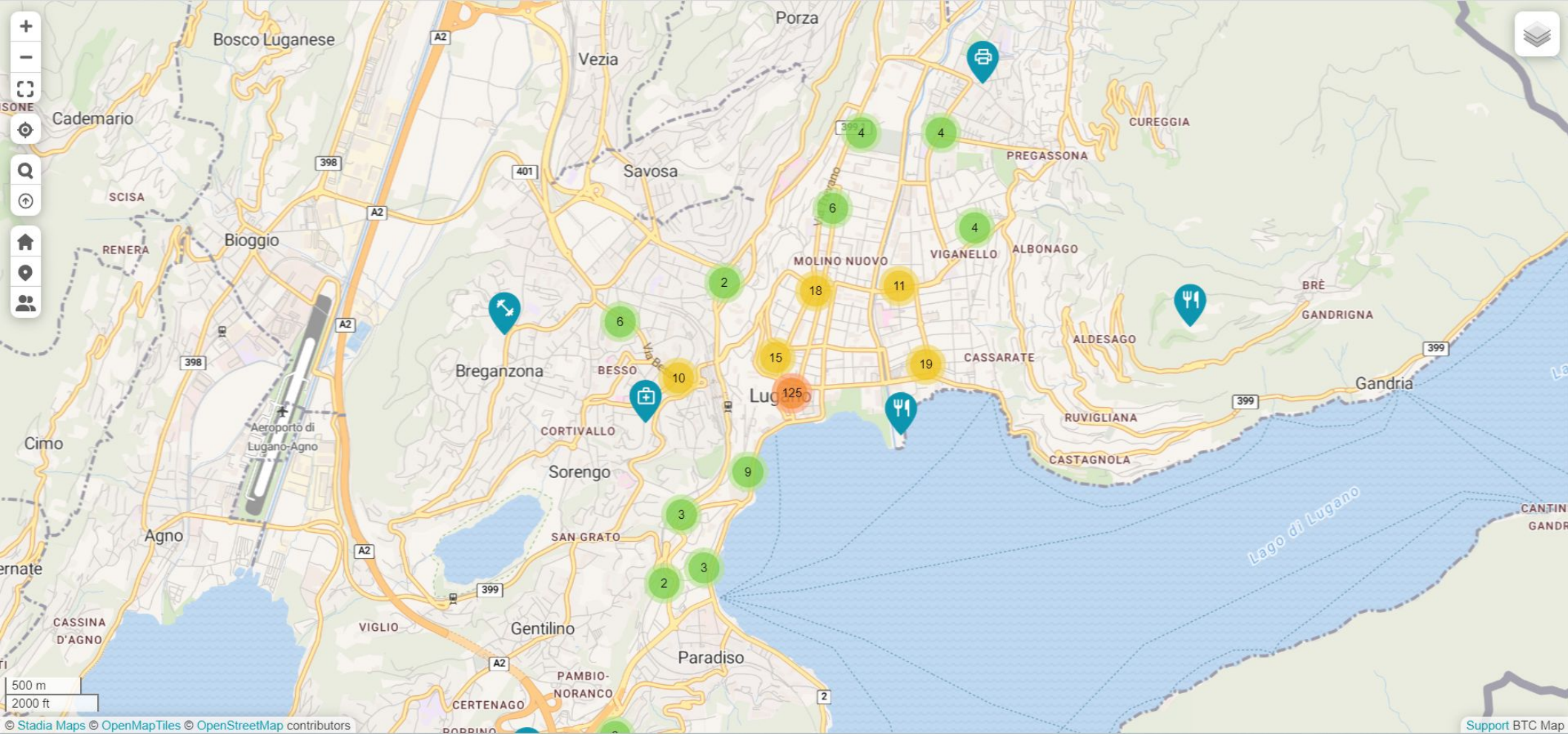
- Si vous recherchez un bel endroit à visiter, où vous pourrez dépenser des bitcoins et rencontrer d'autres bitcoiners, vous devriez absolument visiter le lac Atitlan.



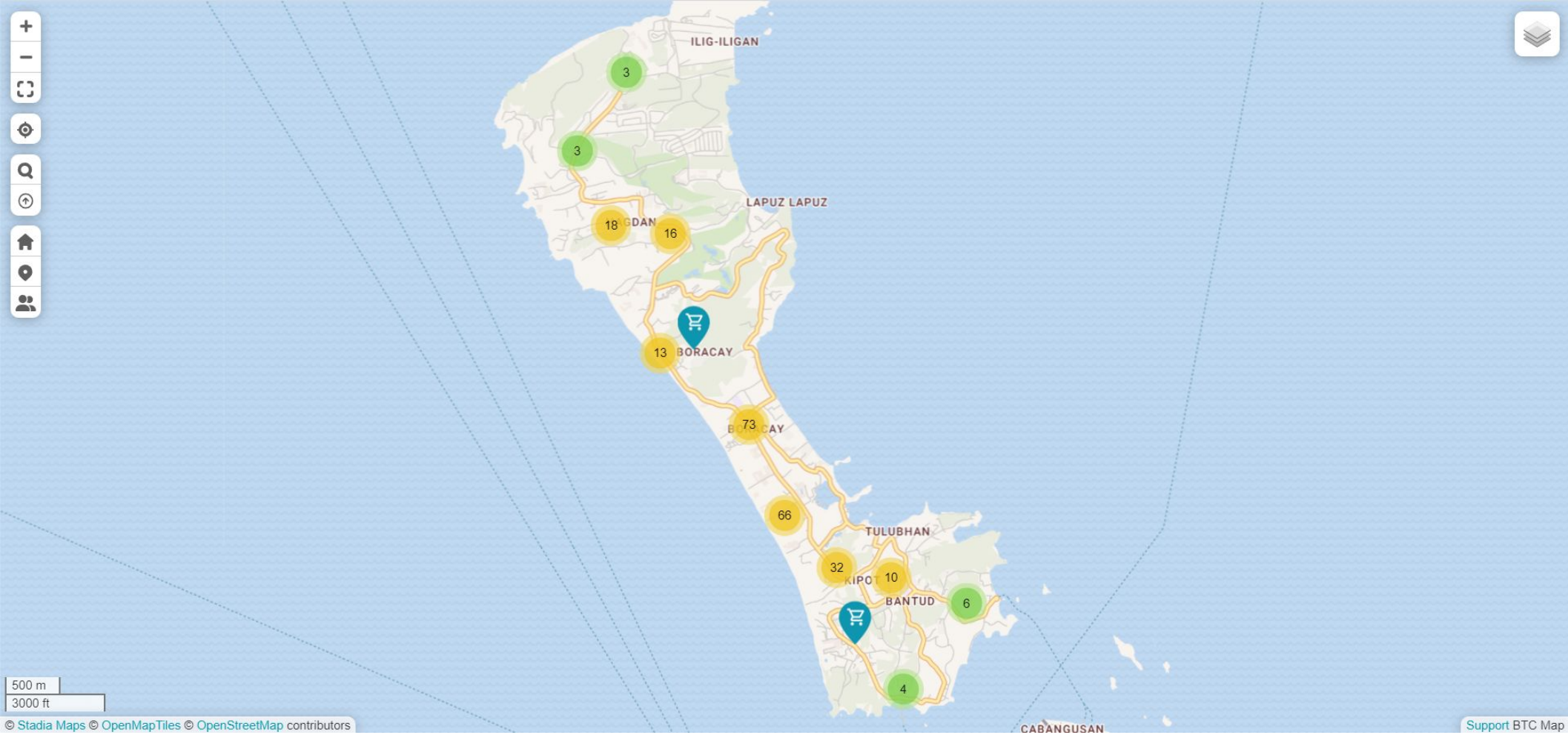

- La prochaine sur la liste est Uvita, une petite ville du Costa Rica un peu plus au sud de l'Amérique centrale. Il est entouré de jungle et se trouve sur la côte Pacifique. Tout comme au Salvador et au Guatemala, cette ville porte un autre nom, Bitcoin Jungle.
- Il existe une grande communauté d’expatriés Bitcoin installés à Uvita. Il est célèbre pour son marché de producteurs, où vous pouvez payer en bitcoin. Ainsi que le festival de la liberté pour Bitcoin et Nostr qui s'y tient désormais.
- L’Amérique centrale pourrait avoir la plus forte concentration d’adoption réelle du bitcoin au monde.




- Nous traversons maintenant l'océan vers l'Afrique. L'Afrique du Sud utilise beaucoup de Bitcoin, principalement concentrée au Cap et à Pretoria, mais également le long de la côte. L'Afrique du Sud et le Nigeria sont les pays d'Afrique où l'adoption du Bitcoin est la plus répandue.
- Il existe un projet d'économie circulaire appelé Bitcoin Ekasi, situé à Mossel Bay, près de George (là où se trouve le cercle jaune avec 30). De nombreux utilisateurs de Bitcoin en Afrique ne sont pas bancarisés et ne peuvent pas faire de commerce international. Bitcoin aide à résoudre ce problème.
- Le Cap accueillera également la conférence Adopting Bitcoin 2024.

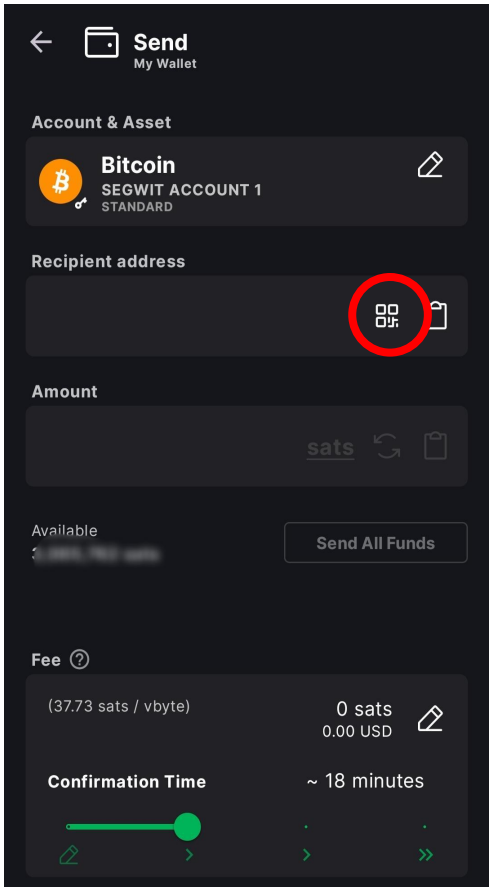



- Passons maintenant à un exemple européen d'endroit où dépenser du Bitcoin, la ville de Lugano en Suisse. C’est probablement la ville la plus favorable au Bitcoin en Europe, encore plus que Berlin.
- Des centaines d’entreprises acceptent le Bitcoin, et de nombreuses sociétés internationales Bitcoin sont basées en Suisse. La Suisse est célèbre pour son secteur bancaire et financier progressiste et innovant.
- Lugano est une belle ville au pied des Alpes et constitue un endroit idéal à visiter pour explorer l’adoption mondiale du Bitcoin.



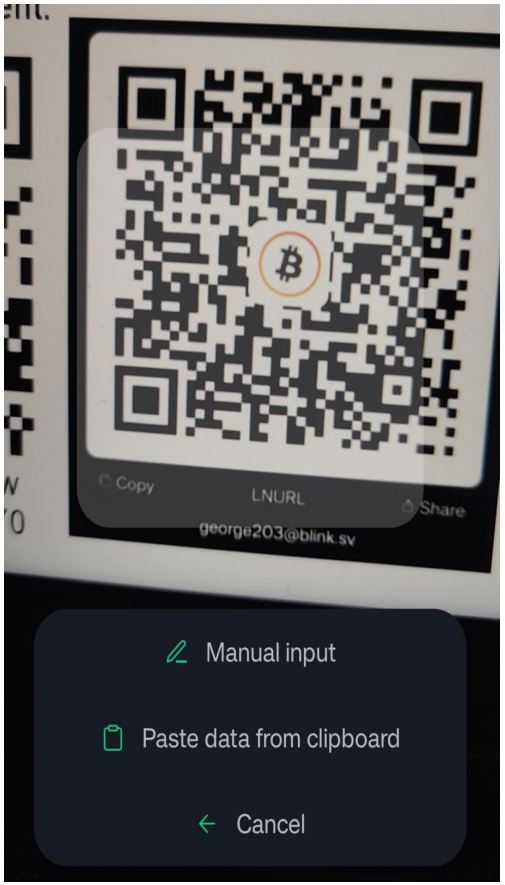

- Ceci est notre dernier exemple de hub Bitcoin BTCMap. L'île tropicale de Boracay aux Philippines, à côté de l'île de Panay. C’est peut-être l’endroit le plus convivial pour les bitcoins de toute l’Asie.
- Il existe de nombreux endroits où dépenser du bitcoin à Boracay, comme des bars, des restaurants et des épiceries.
- Boracay possède également une communauté d'expatriés Bitcoin décente, composée de personnes du monde entier.
- Il sera intéressant de voir comment cette petite île affectera le reste du pays.

# Effectuer des paiements

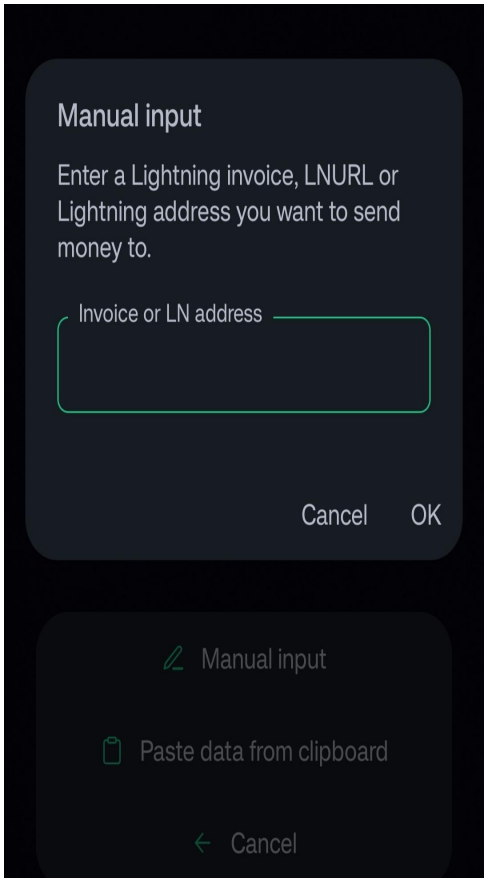



Exemple avec Green Wallet en couche 1 : recherchez le bouton d'envoi dans votre portefeuille et il vous amènera à la page de transfert. Ici, vous pouvez coller ou saisir manuellement une adresse ou appuyer sur le bouton QR, entouré ci-dessus en rouge.


Ci-dessus se trouve la page du scanner QR de Green Wallet. Dirigez l'appareil photo vers le code QR de couche 1 auquel vous souhaitez envoyer des sats. Cela collera l'adresse dans le champ du destinataire de la page de transfert précédente.




Exemple avec Phoenix Lightning : recherchez et appuyez sur le bouton d'envoi et l'écran ci-dessus apparaîtra. Ceci est la page de scanner QR, pointez votre appareil photo sur le code QR Lightning et il le collera dans votre champ de destinataire.




Ou vous pouvez coller une facture Lightning avec le bouton « Coller les données du presse-papiers ». Alternativement, vous pouvez sélectionner « saisie manuelle » et la page ci-dessus s'affichera, où vous pourrez saisir une facture LN ou une adresse Lightning, qui ressemble à une adresse email.

# Acheter du bitcoin

- Nous avons enfin atteint le point où il est temps d'apprendre à réellement acheter du bitcoin. Cela a été volontairement laissé pour la fin, afin de vous assurer de comprendre ce qu'est le bitcoin, pourquoi il est important et comment le conserver vous-même en toute sécurité. De cette façon, vous êtes moins susceptible de paniquer et de vendre votre bitcoin en raison de la volatilité. Plus vous comprenez dans quoi vous investissez, plus il sera facile de le conserver à long terme et, dans le cas des bitcoins, plus il sera également sûr.
- Il existe des centaines d'endroits où acheter des bitcoins dans le monde, et nombre d'entre eux ne sont peut-être pas accessibles, selon l'endroit où vous vivez. L'Amérique du Nord et l'Europe disposent du plus grand choix d'échanges Bitcoin, avec des liens efficaces vers les comptes bancaires pour les dépôts et les retraits. D'autres régions du monde sont plus limitées, vous devrez faire quelques recherches pour savoir exactement quels échanges sont disponibles pour vous et lesquels sont les plus populaires/recommandés.
- Je couvrirai une gamme variée d'échanges disponibles dans le monde entier au cours des prochaines diapositives.
- Voici 5 des plus grandes bourses au monde: Binance, Coinbase, Kraken, OKX, Bitfinex. À mon avis, ce sont de bonnes options, mais ce ne sont pas les meilleures options, mais selon l'endroit où vous vivez, l'une d'entre elles peut être votre seul choix. Parmi ces 5, Kraken serait ma suggestion.




- Mes recommandations d'échange, sans ordre particulier, sont les suivantes (elles peuvent ou non être disponibles pour vous, vous devrez les rechercher ou les tester pour le savoir) :
    - Relai (no KYC, BTC only, Lightning) – Europe/UK – 0.5% off fees code: GEORGEBTC
    - Swan (BTC only, free withdrawals) - US
    - Strike (BTC only, Lightning) – US and others
    - CashApp (BTC only, Lightning) - US
    - CoinCorner (BTC only, Lightning) – UK/Dubai
    - Nexo - Global
    - Gemini - Global
    - Peach (P2P, no KYC, BTC only) - Global
    - RoboSats (P2P, no KYC, BTC only) - Global
    - Bitaroo (BTC only) – Australia/Europe
    - BullBitcoin (no KYC, BTC only, Lightning) – Canada/Costa Rica
    - Bitso – Mexico/Latin America
- Vous connaissez désormais 17 bourses différentes qui vendent du bitcoin, ainsi que leurs différentes exigences/fonctionnalités. Vous devez déterminer quel travail vous convient et combien ils vous factureront en frais. Si possible, je vous recommande d'essayer d'acheter sur un échange sans KYC pour protéger votre vie privée. Et celui qui concerne uniquement le bitcoin, car ils sont moins susceptibles de faire faillite ou de prendre des décisions irresponsables. Comme nous l'avons mentionné à plusieurs reprises auparavant, une fois que vous disposez d'une quantité décente de Bitcoin pour créer un UTXO, vous devriez vous retirer en auto-garde. Soit sur le bitcoin L1, soit sur le réseau Lightning, que plusieurs de ces échanges ont intégré, rendant les retraits plus rapides et moins chers. La plupart de ces échanges disposent d’applications mobiles dédiées, ainsi que de sites Web.

- Si vous ne savez pas comment utiliser réellement ces échanges/applications, recherchez sur YouTube l'échange spécifique que vous souhaitez utiliser, il existe déjà de nombreux guides. Tous les échanges ne fonctionnent pas exactement de la même manière, mais vous trouverez ci-dessous un guide général pour acheter via une application d'échange.

1. Envoyez de l'argent de votre compte bancaire vers le compte d'échange que vous avez créé, soit via un virement bancaire, soit en utilisant un service de connexion intégré à l'application, l'échange doit avoir des instructions complètes sur la façon de procéder. Certains vous permettent également d'utiliser votre carte de crédit/débit directement pour acheter (cependant, cela entraîne généralement des frais supplémentaires).
2. Suivez les instructions des applications d'échange pour échanger vos €/$/CHF/etc contre du BTC (bitcoin). Vous devriez maintenant avoir du bitcoin dans l'application d'échange, qui ne vous appartient pas encore entièrement (à l'exception des échanges comme Relai et Peach, qui vous permettent de détenir vos propres clés et de ne pas en avoir la garde pour vous).
3. Vous devrez maintenant configurer votre portefeuille Bitcoin et noter votre phrase de récupération secrète.
4. Dans votre nouveau portefeuille Bitcoin, recherchez l'endroit où il est indiqué de recevoir et de copier l'adresse, celle-ci doit être une longue chaîne de lettres et de chiffres (dans la plupart des cas, cette adresse commence par « bc », mais pas toujours).
5. Retournez à l'application d'échange et trouvez le bouton de retrait, collez l'adresse, vérifiez qu'elle correspond à celle de votre application de portefeuille, puis appuyez sur envoyer. Si vous envoyez un montant qui est important pour vous et que vous n'avez pas d'expérience en matière de transferts, je vous recommande fortement de faire d'abord un transfert test avec un très petit montant (rappelez-vous que cela peut finir par être un UTXO inutilisable, mais c'est mieux que faire une erreur et perdre une somme plus importante).
6. Le délai de réception de votre bitcoin peut varier considérablement ici, en fonction de la rapidité avec laquelle l'échange lance la transaction et de l'occupation de la blockchain à ce moment-là. Attendez-vous à 10 minutes jusqu’à quelques heures (les transferts réseau Lightning ne prennent que quelques secondes à quelques minutes, cela nécessite cependant un portefeuille Bitcoin Lightning).

# Liste de lecture

- Il existe de nombreux livres sur le Bitcoin disponibles à lire, il peut être un peu difficile de savoir lesquels en valent la peine. J'ai donc dressé une liste de livres sur le bitcoin ou sur le bitcoin qui peuvent approfondir votre apprentissage et vous envoyer plus profondément dans le terrier du lapin.
    - L'histoire de Bitcoin:
        - (FR) Le Livre de Satoshi – Phil Champagne
        - The Blocksize War – Jonathan Bier
        - The Genesis Book – Aaron Van Wirdum
        - Layered Money – Nik Bhatia
    - La finance de Bitcoin:
        - (FR) L'étalon Bitcoin – Saifedean Ammous
        - Broken Money – Lyn Alden
        - The Price of Tomorrow – Jeff Booth
        - The Creature from Jekyll Island – G. Edward Griffin
        - Big Debt Crisis – Ray Dalio
        - (FR) L'individu souverain - William Rees-Mogg and James Dale Davidson
    - Aspects techniques de Bitcoin:
        - (FR) Au coeur de Bitcoin – Andreas Antonopoulos
        - Programming Bitcoin – Jimmy Song

# Ressources

***Tous les liens sont en anglais:***

- ***Pour en savoir plus sur ce qu'est l'argent:*** Cliquez ici
- ***Graphique de la dette du gouvernement américain:*** Cliquez ici
- ***Plus de statistiques sur la dette:*** *Cliquez ici*
- ***Comprendre comment le plafond d'approvisionnement de 21 millions est appliqué:*** Cliquez ici
- ***Informations sur le calendrier d'approvisionnement de Bitcoin:*** Cliquez ici
- ***Graphique de croissance du PIB mondial:*** *Cliquez ici*
- ***Lisez un article du conseil minier Bitcoin sur le mix énergétique du Bitcoin:*** Cliquez ici
- ***Un graphique montrant l'historique du taux de hachage Bitcoin:*** *Cliquez ici*
- ***Liste de mots des phrases de départ BIP39:*** *Cliquez ici*
- ***Liste de Jameson Lopp des attaques physiques Bitcoin signalées dans l'actualité:*** *Cliquez ici*
- ***Apprenez-en davantage sur les clauses restrictives, comment elles aident Bitcoin et qui les soutient:*** *Cliquez ici* ***&*** *ici*
- ***Un lien pour télécharger le logiciel Bitcoin Core Node:*** *Cliquez ici*
- ***Le site Web de Start9, une suite logicielle de nœuds Bitcoin:*** *Cliquez ici*
- ***Et le site Web d'Umbrel, une autre suite logicielle de nœuds Bitcoin:*** *Cliquez ici*

# Liens: portefeuilles et plaques de gravure

- Blockstream Jade Hardware Wallet
- Coinkite Coldcard Hardware Wallet
- Foundation Passport Hardware Wallet
- Bitbox Hardware Wallet
- Seedsigner DIY Hardware Wallet
- Blockstream Green Software Wallet
- Sparrow Software Wallet
- Electrum Software Wallet
- Casa Collaborative Multisig Wallet
- Unchained Collaborative Multisig Wallet
- Phoenix Lightning Wallet
- Breez Lightning Wallet
- Jameson Lopp's List of Steel Seed Backup
- www.Seedsafe.io plaque métallique avec poinçon

# Outils utiles

***Outils:***

- Clark Moody Bitcoin Info Dashboard
- Trading View Price Charts
- Jameson Lopp's Website
- Wicked's Bitcoin Tutorials
- Mempool.space Block Explorer
- Sparrow Wallet's Amazing FAQs
- Bitrefill: Buy Giftcards With Bitcoin Referral Code: ioxzotvy
- The Bitcoin Company: Buy Giftcards With Bitcoin Referral Code: LSG1YN
- Satsback: Get Sats Back When Shopping Online

# Fin !

Toutes nos félicitations! Vous êtes arrivé à la fin du cours, j'espère que vous l'avez apprécié et que vous avez beaucoup appris. Assurez-vous de consulter les liens sur la page de ressources si vous souhaitez continuer à en apprendre davantage sur Bitcoin et mieux comprendre certains des sujets que nous avons abordés dans ce cours.
N'hésitez pas à me suivre sur Twitter **@George203BTC** et n'oubliez pas de me faire savoir ce que vous avez pensé de ce cours !
Si vous avez apprécié le cours, j'apprécierais vraiment tout don ! Vous trouverez ci-dessous les codes QR et les adresses pour Bitcoin. De gauche à droite : couche 1, Lightning et Liquid. Et n'hésitez pas à partager le cours avec toute personne qui, selon vous, en bénéficiera ! Votre partenaire, un ami, voire un grand-parent.
Traduction vers le français par **@bitcoin_valais** (https://bitcoinvalais.ch/) et @noufsmith

bc1qyxy2v695dsptcjz0w
w0uxq5wzkpf48ldrfm370


lq1qqd2ysf43xfkrpm22avhrs8dqk5smqq87
np773j95fmmuzktq5shfka5ap66wpwnkccv
znsqtj82gwp94gxa9q36la47qxkj3h