



BITCOINMETZ
ANTI-CBDC

LIGHTNING NETWORK ⚡

Le réseau Lightning, la solution au passage à l'échelle de Bitcoin

Atelier Lightning #1 - Introduction à Lightning Network.

Premiers pas : Comprendre, installer, tester.



LIGHTNING #1

SOMMAIRE

De la théorie à la pratique, c'est parti !
Pas à pas, pour tout comprendre.

Qu'est-ce que Lightning Network ?

- 1.1. Pourquoi le réseau Lightning est né ? 03
- 1.2. Comment fonctionne Lightning ? 05
- 1.3. Avantages et limites de Lightning 06

Comment utiliser Lightning ?

- 2.1. Prérequis 08
- 2.2. Mettre en place un portefeuille Lightning 08
- 2.3. Conseils et bonnes pratiques 09

À vous de jouer !

- 3.1. Téléchargez Phoenix Wallet 10
- 3.2. Envoyer / Recevoir un paiement 11

Aller plus loin

- 4.1. Exemples d'usages 11

QU'EST CE QUE Lightning Network ?



1.1. Pourquoi le réseau Lightning est né ?

Dès 2013, avec l'augmentation significative du nombre de transactions effectuées sur le réseau, de nombreux débats ont émergé quant au besoin d'augmenter la taille des blocs de Bitcoin pour confirmer plus de transactions simultanément, notamment pour ne pas freiner l'adoption de Bitcoin pour le plus grand nombre.

En effet, les blocs dans lesquels sont intégrées les transactions ne peuvent pas dépasser une taille de 1MB et ne sont validés qu'à un intervalle de 10 minutes environ. En moyenne, cela correspond à environ 7 transactions traitées par seconde (contre 24 000 pour le réseau Visa*). Cependant, il ne s'agit pas d'une mauvaise conception mais bien une caractéristique voulue par Satoshi Nakamoto, son fondateur.

Néanmoins, dans le cadre d'une adoption croissante, cette conception ne permet pas aux individus d'effectuer des paiements et micro-paiements pour des achats quotidiens à faibles frais.

En 2015, Joseph Poon et Thaddeus Dryja ont publié leur livre blanc sur le réseau Lightning, une surcouche au-dessus du réseau Bitcoin natif qui permet de répondre à la problématique présentée. Lancé en août 2017, le réseau Lightning connaît depuis une adoption croissante.

A l'inverse des altcoins qui ont tenté d'augmenter leur capacité transactionnelle en modifiant directement leur architecture réseau, le passage à l'échelle de Bitcoin se fait via un réseau off-chain qui n'impacte pas la sécurité et la distribution de son réseau principal.

Pour en savoir plus sur ce débat, on vous conseille le livre "La Guerre des Blocs" de Jonathan Bier.

*À proprement dit, le réseau Visa ne traite pas des transactions mais des autorisations de transactions.



1.2. Comment fonctionne Lightning ?

Explication technique

Le réseau Lightning est un réseau de seconde couche, qui s'appuie sur le réseau primaire Bitcoin. Il repose sur l'établissement de canaux de paiements bidirectionnels interconnectés qui permettent d'effectuer des transactions avec une rapidité d'exécution, une meilleure confidentialité et de moindres frais que le réseau primaire.

Un canal entre deux nœuds est ouvert par le biais d'une transaction engageant un certain montant de Bitcoins bloqué dans une adresse multi-signature, dont le contrôle requiert l'accord commun des deux parties. Lors de l'ouverture, l'utilisateur initiant la transaction choisit s'il ouvre un canal public ou privé avec son partenaire et détermine le nombre de Bitcoins initialement bloqué dans le canal.

Une fois ouvert, les participants peuvent effectuer un nombre illimité de transactions à faible coût, entre eux, dans la limite du montant bloqué dans le canal, sans devoir diffuser chaque échange sur le réseau primaire. Chaque nouvelle transaction met à jour les soldes des deux parties et remplace l'état précédent (appelé transaction d'engagement).

Ainsi, le réseau Lightning devient un maillage de canaux interconnectés, permettant à chaque participant d'envoyer des Bitcoins à n'importe qui sur le réseau sans qu'il n'y ait de canal de paiement partagé préétabli. L'acheminement transite par des canaux intermédiaires qui, sur base de techniques cryptographiques telles que les HTLC, n'ont pas accès aux fonds lors du transfert.

Lorsqu'une des deux parties décide de clôturer le canal, une transaction est publiée sur le réseau primaire avec l'état final du canal (cf. la transaction d'engagement, c'est-à-dire ce que possède chaque partie) permettant l'enregistrement final des échanges. La fermeture du canal est finalisée une fois que la transaction de clôture est confirmée dans un bloc.

Métaphore

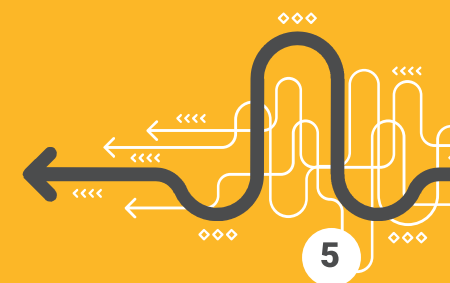
Si le réseau primaire Bitcoin est un autoroute où circulent voitures et poids lourds, le réseau Lightning représente le réseau de petites routes départementales qui relient villes et villages ensemble.

Deux mairies s'accordent pour créer une route reliant leurs deux villes, elle-même connectée à l'autoroute nationale. L'accord ne tient que si les deux mairies acceptent et celui-ci est publié.

Les automobilistes peuvent utiliser la route entre les deux villes à volonté, sans devoir passer par l'autoroute qui est payante à chaque passage.

En développant un réseau de routes entre chaque ville, les individus peuvent effectuer des trajets sans nécessairement avoir besoin de passer par l'autoroute ni avoir l'accord de toutes les mairies par lesquelles ils passent.

Si l'une des deux mairies décide de clôturer la route entre les deux villes, les deux mairies font état du bilan des dépenses de chacune pour cette route et effectuent une procédure de clôture pour informer le réseau routier en amont.



1.3. Avantages et limites de Lightning Network

LES AVANTAGES

Rapidité :

À l'inverse du réseau primaire, le réseau Lightning permet d'effectuer des transactions entre individus quasi-instantanément. Les transactions n'ont pas besoin d'être confirmées dans des blocs pour être effectives. Une fois que le destinataire reçoit son paiement, la transaction est considérée comme confirmée (délai de quelques secondes).

Passage à l'échelle :

En bénéficiant de transactions quasi-instantanées, le réseau Lightning est adapté pour un usage massif de plusieurs millions, voire milliards d'utilisateurs, capable de traiter plusieurs milliers de transactions à la seconde. Du fait que les transactions sont valides tant qu'il y a suffisamment de liquidités et de canaux ouverts entre les différentes parties, il est possible d'étendre son usage à un plus grand nombre.

Faibles coûts :

Comme les transactions ne sont pas incluses dans des blocs, quasiment aucun frais n'est appliqué. Seuls les frais

de routage sont appliqués sur le réseau Lightning, c'est-à-dire que les utilisateurs paient un frais aux nœuds par lesquels passent leur paiement. La majorité du temps celui-ci équivaut à moins d'1% du montant de la transaction (contre 3% pour les frais de carte bancaire). À l'inverse du réseau primaire, les frais sur Lightning vont être proportionnels à la quantité envoyée et au pourcentage de frais fixés par les nœuds de routage. Cette méthode se prête parfaitement à l'envoi de petits montants pour des dépenses quotidiennes.

Confidentialité :

Hormis les transactions d'ouverture et de fermeture de canaux qui sont publiquement consultables sur le réseau primaire, il est impossible de tracer sur le réseau Lightning les différents paiements effectués au sein d'un canal. Même si ce paiement passe par des nœuds intermédiaires, ces derniers n'ont pas connaissance de l'expéditeur initial et du destinataire final. Également, il est aussi possible d'ouvrir des canaux privés qui permettent des échanges sans que le reste du réseau ne soit au courant.



LES INCONVÉNIENTS

Adoption limitée :

Contrairement au réseau primaire, moins d'utilisateurs et de services utilisent actuellement Lightning (~4000 BTC de liquidité). Certains portefeuilles, comme GreenWallet, Sparrow ne permettent pas d'effectuer des transactions sur Lightning. Cela nécessite de télécharger un portefeuille dédié tel que Phoenix Wallet, Zeus Wallet ou un supportant le réseau primaire et Lightning (ex : BlueWallet, Muun Wallet, Electrum).

Gestion des canaux :

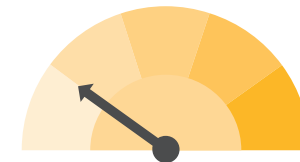
Le réseau Lightning repose sur un maillage de canaux de paiements entre nœuds interconnectés. Par conséquent, dans le cas où l'utilisateur gère lui-même ses canaux de paiement, il est nécessaire de s'assurer que la liquidité est correctement répartie pour réaliser ou recevoir le paiement souhaité. Cette contrainte est d'autant plus importante si le nœud agit comme nœud de routage sur le réseau. Cependant, si l'utilisateur utilise un service de gardiennage (ex : Wallet of Satoshi) cette contrainte est directement gérée par le fournisseur de service.

Connexion à Internet permanente :

Que ce soit pour effectuer/recevoir un paiement ou router de la liquidité, l'utilisateur doit être connecté à Internet. Contrairement au réseau primaire, l'expéditeur et le destinataire communiquent une suite de messages pour que le paiement puisse se réaliser sur le réseau Lightning (appelés HTLC pour Hash Time Locked Contracts), ce qui nécessite une connexion permanente à Internet. Il existe certaines alternatives (ex : les cartes NFC) qui comportent moins de fonctionnalités qu'un portefeuille Lightning classique.

Apprentissage nécessaire :

Ayant son propre fonctionnement, différent du réseau primaire, le réseau Lightning requiert un apprentissage supplémentaire si l'utilisateur souhaite être en maîtrise des outils mis à disposition. Cependant, il existe des portefeuilles et solutions simplifiées (ex : Wallet of Satoshi, LNBits, PeerSwap) qui permettent de simplifier ou de s'affranchir de certaines contraintes d'usage (gestion des canaux et de la liquidité, sauvegarde des états, connexion du nœud, etc.).



COMMENT UTILISER Lightning Network ?



2.1. Prérequis



2.2. Mettre en place un portefeuille Lightning



USAGE SIMPLIFIÉ

1 TÉLÉCHARGER UNE APPLICATION

Se rendre sur un site officiel pour télécharger une application de portefeuille Lightning (Phoenix Wallet, Muun Wallet, Breez Wallet...)

2 CRÉER UN PORTEFEUILLE

Ouvrir l'application. Un portefeuille est automatiquement créé à la première ouverture.

3 SAUVEGARDER LA SEED PHRASE

Une phrase de 12 mots apparaît : conservez-la en sécurité. Elle est indispensable pour récupérer vos fonds si vous perdez votre téléphone.

4 RECEVOIR DES SATOSHIS

- Depuis une facture à usage unique (Bolt11).
- Depuis une facture à usage multiple (Bolt12, pour plus de confidentialité et pratique pour les commerçants).
- Depuis une transaction sur le réseau primaire (non possible avec son propre nœud).

8



Un smartphone
connecté à Internet



Une application de portefeuille
supportant Lightning



De la liquidité pour ouvrir un canal
(recommandé 150 000 sats)

Phoenix Wallet



Muun Wallet



Breez Wallet



USAGE COMPLET

1 UN SMARTPHONE / ORDINATEUR

Connecté à Internet.

2 UN NŒUD BITCOIN

Connecté à Internet (toujours).

3 UNE APPLICATION LIGHTNING

Pour la gestion du nœud sur
Lightning, (voir QR Code ci-dessous).

4 LIQUIDITÉ À PRÉVOIR

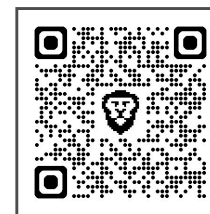
Pour ouvrir un canal
(recommandé 150 000 sats).



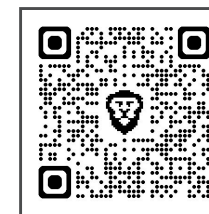
Core Lightning



Ride the Lightning



Blue Wallet LN



LNBits

2.3. Conseils et bonnes pratiques



Conseil #1

Sauvegarder sa seed phrase
sur un support hors-ligne et à
l'abri de tous.



Conseil #2

Ne pas utiliser Lightning pour stocker la
majorité de ses Bitcoins, Lightning est conçu
pour les paiements (max. 500€ conseillé).



Conseil #3

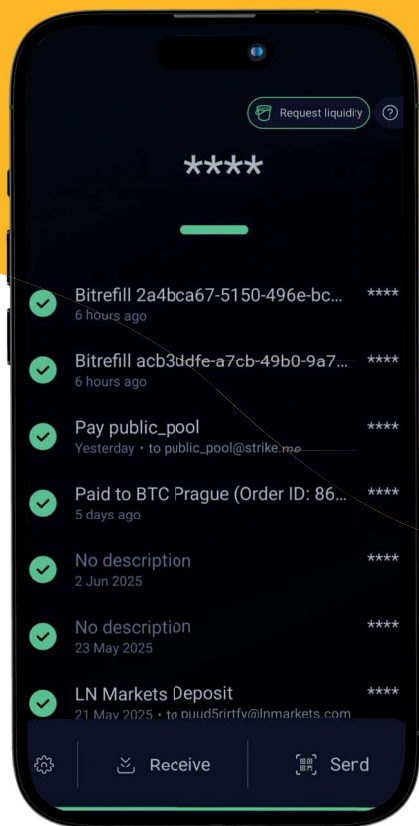
Surveiller l'équilibre de ses canaux
si beaucoup de transactions
entrantes ou sortantes.



Conseil #4

Avec son propre nœud, toujours
effectuer une sauvegarde de l'état
du canal après une transaction.

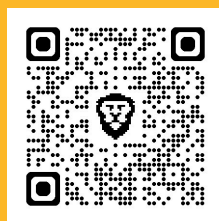
9



À VOUS DE JOUER ! Faites chauffer les sats



3.1. Téléchargez Phoenix Wallet



1. ÉCRAN D'ACCUEIL

Après avoir créé un portefeuille et sauvegardé votre seed phrase, vous arriverez sur cette interface d'accueil.



2. MONTANT

Le montant disponible est indiqué en haut, au centre. Vous pouvez cacher le montant en cliquant dessus. Des étoiles apparaissent (voir photo ci-dessus).



3. TRANSACTIONS

Vous pouvez visualiser ici, l'historique de toutes vos transactions. Elles apparaissent les unes en dessous des autres.

3.2. Envoyer / Recevoir un paiement



ALLER PLUS LOIN Quelques exemples



4.1. Exemples d'usages

- **Bitrefill** : Achats de cartes cadeaux.
- **BTC Map** : Dépensez chez des commerçants autour de vous.
- **Mullvad VPN** : Service de VPN.
- **Mt Pelerin** : Achat et vente de Bitcoin.
- **LN Markets** : Plateforme de produits financiers dérivés sur Bitcoin.





BITCOINMETZ
ANTI-CBDC

MEETUP LOCAL & COMMUNAUTAIRE

Contacts :

bitcoinmetz.fr

btcmetz@protonmail.com

REJOIGNEZ-NOUS !

