INSTITUT SAPIENS

Comprendre le Lightning Network

Note — Juin 2020

Table des matières

À propos de l'auteur

Yorick de Mombynes

Haut fonctionnaire et chercheur associé à l'Institut Sapiens

Né en 1975, diplômé de l'École Supérieure de Commerce de Paris (ESCP) et de l'Institut d'Études Politiques de Paris (IEP), titulaire d'une licence de philosophie de l'Université Sorbonne Paris IV, ancien élève de l'École Nationale d'Administration (ENA), il a été conseiller technique du premier ministre François Fillon et a travaillé chez Total. Il a enseigné l'économie et la philosophie politique à l'IEP de Paris. Il est conseiller référendaire à la Cour des comptes.

A propos de l'Institut Sapiens

L'Institut Sapiens est la première « think tech » française. Organisme indépendant à but non lucratif, sa vocation est de peser sur le débat économique et social français par la diffusion de ses idées. Il innove par ses méthodes, son ancrage territorial et la diversité des intervenants qu'il mobilise, afin de mieux penser les enjeux vertigineux du siècle.

Sapiens souhaite défendre la place de l'humain dans une société bouleversée par le numérique. Son axe principal de travail est l'étude et la promotion des nouvelles formes d'écosystèmes favorables au développement économique et au bien-être social.

Sapiens fédère un large réseau d'experts issus de tous horizons, universitaires, avocats, chefs d'entreprise, entrepreneurs, hauts fonctionnaires, autour d'adhérents intéressés par le débat touchant aux grands enjeux actuels.

Plus d'informations sur **http://institutsapiens.fr**

INSTITUT SAPIENS

Introduction

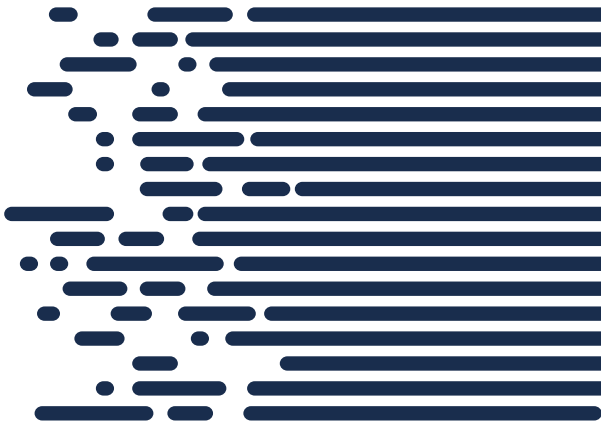
Comme l'avaient pressenti ses premiers utilisateurs, les caractéristiques techniques du système Bitcoin font qu'il peut difficilement servir de réseau de paiement universel. Il est davantage un protocole d'enregistrement décentralisé de transactions qu'un moyen de paiement.

Le Lightning Network est un protocole qui complète celui de Bitcoin pour lui permettre de dépasser ses limitations. C'est un dispositif qui rend possible des transactions instantanées, anonymes, de montants éventuellement très réduits, pour des frais négligeables, et sans consommation additionnelle d'énergie.

Il fonctionne normalement depuis 2018. Son développement informatique comme sa facilité d'utilisation ont connu une nette accélération depuis mi-2019. Il a le potentiel de transformer radicalement l'industrie du paiement et même une partie du secteur financier, tout en contribuant à la diffusion et à la massification du système Bitcoin.

Cette note a pour objet de résumer les grandes caractéristiques du réseau Lightning (I), ses principes techniques (II) et son fonctionnement économico-financier (III).

NB : rédigée par un non-technicien à l'attention de non-techniciens, cette note est nécessairement très imparfaite. Elle l'aurait toutefois été bien davantage sans le feed-back technique précieux de Pierre-Marie Padiou, Julien Guitton, Marco et Sosthène, que l'auteur tient ici à remercier.



I - Présentation générale

A) Concept

Lightning est un protocole *open source* qui assure le passage à l'échelle (« scalabilité ») de Bitcoin. Il permet d'augmenter le nombre de transactions possibles par seconde, pour des montants transférés éventuellement très faibles, pour un coût réduit pour les utilisateurs, de manière plus confidentielle et sans dégrader excessivement le niveau de sécurité du système. Cette technologie est aussi utilisable pour certaines autres cryptomonnaies mais c'est seulement Bitcoin qui est ici évoqué.

Le réseau Lightning permet de réaliser des transactions en bitcoins mais en dehors de la blockchain (off-chain). Après une mise sous séquestre initiale de fonds sur la blockchain *(on-chain),* ne sont enregistrées ponctuellement sur cette dernière que le solde des transactions ajoutées les unes aux autres. Ce réseau fonctionne comme une accumulation de chambres de compensation, en agrégeant différentes positions d'achat et de vente de bitcoins.

Le fait d'effectuer ces transactions hors de la blockchain permet d'éviter les lourdeurs que cette dernière implique (vérification par tous les nœuds, temps de confirmation, frais de transaction, dépense énergétique du minage). Et le fait d'enregistrer sur Bitcoin le solde des transactions entre elles permet de bénéficier de l'inviolabilité de la blockchain. Ce sont ces deux avantages qui sont recherchés dans le même dispositif.

Lightning est donc un réseau de paiement qui se superpose à Bitcoin tout en lui étant relié. On le décrit comme une « surcouche », une « couche secondaire », un *layer 2* (Bitcoin étant le *layer 1).*

Cette surcouche ne fait pas peser de risque technique supplémentaire à Bitcoin et à ses utilisateurs. Si le réseau Lightning rencontrait un problème systémique insurmontable, ses utilisateurs pourraient récupérer tous leurs fonds immédiatement et facilement en publiant sur la blockchain Bitcoin la dernière mise à jour de leurs transactions Lightning.

Enfin, Lightning permet un passage à l'échelle de Bitcoin sans augmenter sa consommation énergétique. En effet, les transactions qu'il permet ne nécessitent pas de minage par la preuve de travail, qui est la composante du système Bitcoin

nécessitant des calculs informatiques massifs et une forte consommation d'électricité.

Tout l'objet du protocole Lightning est de de faire fonctionner ce système de paiement novateur de manière satisfaisante, notamment en préservant la confidentialité de ses utilisateurs et en limitant tout risque de vol.

B) Historique

Hal Finney, l'un des premiers interlocuteurs de Satoshi Nakamoto, évoquait dès 2010 la nécessité d'un *layer 2* pour assurer la scalabilité de Bitcoin. Et Nakamoto avait théorisé la brique de base qui a ensuite conduit au Lightning. Diverses idées de réseau de paiement hors-chaîne ont circulé à partir de 2011.

En 2015, deux jeunes chercheurs, Joseph Poon et Thaddeus Dryja, ont présenté le concept théorique du Lightning Network avant d'en publier une version plus aboutie en 2016, pendant qu'un développeur, Rusty Russel proposait des modalités de mise en œuvre concrète.

Dans les années qui ont suivi, trois startups se sont attelées au développement du protocole : Acinq (société française dont l'un des actionnaires est BPI France), Lightning Labs et Blockstream.

En janvier 2018, après une phase de tests, le réseau a été ouvert au public et la première transaction en bitcoins a eu lieu sur Lightning. Une frise chronologique détaille les étapes de ce protocole à la fois récent et déjà relativement ancien.

C) Gouvernance

Si Bitcoin et Lightning sont tous deux des protocoles *open source*, le premier a été développé exclusivement par des individus bénévoles, alors que le second l'a été à la fois par quelques particuliers et par des entreprises commerciales. Pour éviter une dispersion du projet entre plusieurs réseaux incompatibles, ces dernières se sont mises d'accord dès 2016 sur une dizaine de spécifications techniques. Encore aujourd'hui, elles se coordonnent régulièrement et publient leurs interactions.

Ecrites dans des langages informatiques différents et ne proposant pas exactement les mêmes fonctionnalités, ces différentes implémentations restent interopérables et donnent accès au même

réseau, tout comme des navigateurs différents donnent accès au même Internet.

Ces entreprises se sont engagées dans ce projet parce qu'elles espèrent jouer un rôle dans la nouvelle économie qui pourrait naître de cette technologie, même si leur futur modèle d'affaires n'est pas toujours totalement identifié à l'heure actuelle. Le fait que le protocole soit *open source* garantit en tout cas qu'aucune d'entre elle ne pourra en prendre le contrôle. Et le fait que plusieurs implémentations aient été lancées diminue le risque de faille technique majeure sur l'ensemble du réseau et réduit fortement tout risque de monopole.

Le réseau fonctionne sans anicroche depuis 2018. Son développement est toutefois loin d'être terminé et de nombreuses étapes restent à franchir pour améliorer ses performances et surmonter certains défis techniques redoutables *(cf. infra)*. Les entreprises qui y contribuent ont récemment vu leurs moyens renforcés à travers de nouvelles levées de fonds : 7 M€ en octobre 2019 pour Acinq et 10M€ en février 2020 pour Lighning Labs.

D) Etat du réseau et écosystème

Depuis son ouverture au public au début de l'année 2018, le réseau s'est développé à très grande vitesse. Trois indicateurs permettent d'en mesurer l'étendue actuelle : le nombre de nœuds, le nombre de « canaux de paiements » (notion présentée dans la partie II) et la somme des bitcoins circulant sur le réseau.

Le réseau Lightning est composé de 12 799 nœuds, reliés par 36 633 canaux de paiements abritant une somme total d'environ 948 bitcoins (14 juin 2020). Ces chiffres sont actualisés en temps réel ; des séries temporelles sont aussi disponibles.

Il convient toutefois de souligner que le nombre de nœuds, de canaux de paiement et de bitcoins engagés réellement sur le réseau est plus élevé que ces chiffres car un certain nombre d'acteurs n'ont techniquement pas besoin de révéler leur existence au réseau *(cf. infra).* S'agissant des canaux publics, il n'existe pas de données précises mais ils pourraient représenter environ 72% de l'ensemble des canaux, selon une estimation en janvier 2020. En tout cas l'étendue du réseau est nécessairement plus grande que celle qui est visible et mesurée. Cela permet de relativiser certaines interprétations parfois alarmistes des évolutions de court terme de ces paramètres.

Enfin, tout un écosystème d'entreprises, d'analystes et de chercheurs est en train de se mettre en place autour de Lightning. Le développement de cet écosystème est décrit notamment ici et ici. Par exemple, de plus en plus d'applications conçues spécifiquement pour fonctionner sur Lightning sont lancées. L'une d'entre elles, Tipping.me, permet au lecteur magnanime d'envoyer un pourboire à l'auteur de cette note en utilisant le réseau Lightning.

II - Principes techniques

Les éléments qui suivent sont très simplifiés. Des compléments techniques sont disponibles sur les sites de BitConseil et des développeurs Lightning.

A) Transactions publiables mais non publiées

Lightning est *« un protocole qui permet de mettre à jour des transactions qui sont publiables mais qui ne sont pas publiées ».* Cette définition, apparemment énigmatique, de Fabrice Drouin (CTO d'Acinq), est en fait très éclairante. Il convient d'abord de comprendre en quoi publier chaque transaction en bitcoins sur la blockchain Bitcoin n'est pas efficient.

Sur Bitcoin, c'est l'étape de la publication de la transaction qui déclenche le processus de vérification par les dizaines de milliers de nœuds du réseau, puis de minage par les acteurs chargés d'enregistrer les blocs sur la blockchain. Pour rappel, une transaction en bitcoins est un message qui est « publié », c'est-à-dire diffusé à l'ensemble du réseau Bitcoin : la transaction est alors vérifiée et validée par l'ensemble des nœuds avant d'être enregistrée dans le registre décentralisé et inviolable qu'est la blockchain.

C'est ce processus de « consensus global » qui organise ce système de transfert de valeur à la fois sans tiers de confiance et sans risque de double dépense. C'est lui qui garantit l'exceptionnel niveau de sécurité de Bitcoin, grâce une combinaison originale entre décentralisation et minage par la preuve de travail.

Mais ce processus est extrêmement lourd. Il peut même paraître titanesque et disproportionné pour des transactions de faible montant. Faire vérifier un menu achat par des dizaines de milliers d'ordinateurs répartis sur toute la planète, puis engager une dépense énergétique colossale permettant de la sceller pour l'éternité dans

un registre dupliqué des dizaines de milliers de fois est évidemment excessif. Par ailleurs, ce mécanisme coûte aux utilisateurs des frais de transaction non négligeables, et les transactions ont un délai de confirmation incompressible de plusieurs minutes.

Ce dispositif rend techniquement impossible tout passage à l'échelle (à taille des blocs constante) : il ne permettrait pas, en l'état, à Bitcoin d'atteindre les volumes de transactions des réseaux de paiement traditionnels comme Visa.

Pour surmonter ces difficultés, **c'est donc l'étape de la publication de la transaction que cherche à modifier Lightning.** C'est une solution différente de celle, promue par certains, consistant à augmenter significativement la taille des blocs.

Avec Lightning, les utilisateurs engagent les bitcoins qu'ils veulent se transmettre, mais ne publient pas toutes leurs transactions : seules sont publiées (et donc vérifiées puis enregistrées dans la blockchain) celles qui, ouvrent la possibilité d'échanges entre eux et celles qui, ponctuellement, assurent le règlement des divers échanges ayant eu lieu entre eux sur une certaine période.

Les paiements effectués sont bien des transactions en bitcoins. Ce sont des messages qui ont exactement la même forme, la même structure et le même type de contenu ; la seule différence est que la plupart d'entre eux ne sont pas publiés : ces paiements ne sont pas diffusés sur le réseau Bitcoin. On réalise donc certaines transactions en bitcoins sans avoir besoin à chaque étape du protocole Bitcoin.

Comment ce paradoxe est-il réalisé techniquement ? En mettant en réseau une fonctionnalité imaginée à l'origine pour relier des détenteurs de bitcoins deux à deux : les « canaux de paiements bidirectionnels ». Il convient d'abord de comprendre ce qu'est un canal de paiement, avant de voir comment plusieurs canaux peuvent être interconnectés.

B) Canaux de paiement bidirectionnels

Un canal de paiement est une sorte de compte financier bilatéral entre deux détenteurs de bitcoins qui leur permet de s'échanger des bitcoins et de n'enregistrer dans la blockchain que le solde final de leurs échanges, une fois qu'ils décident de fermer ce compte. Le canal est « unidirectionnel » si c'est toujours le même participant qui envoie des fonds à l'autre, et « bidirectionnel » si les transactions sont réciproques.

Trois étapes peuvent être distinguées.

Premièrement, les deux parties ouvrent un canal de paiement en publiant conjointement sur la blockchain Bitcoin une transaction indiquant combien de bitcoins appartient à chacun au début de l'existence du compte. Une fois validée par le réseau Bitcoin et intégrée dans un bloc, cette transaction se trouve scellée dans la blockchain.

Les fonds sont mis sous séquestre et restent sous le contrôle conjoint des deux participants. Cela se fait grâce à une fonctionnalité permettant de créer des adresses Bitcoin dont le contrôle est partagé par plusieurs clés privées : une signature de chaque partie reste nécessaire pour mouvementer les fonds présents dans le canal.

Deuxième étape : les deux participants s'envoient des transactions pendant la plage de temps de leur choix : ils modifient autant de fois qu'ils le souhaitent la répartition de ces sommes entre eux par consentement mutuel. Ils le font en s'envoyant des transactions libellées en bitcoins mais non publiées sur la blockchain. On pourrait penser qu'il s'agit en fait de « promesses de bitcoins » mais il s'agit bien, techniquement, de bitcoins.

Ces utilisateurs ne sollicitent aucun intermédiaire et ne payent aucun frais de transaction puisqu'ils ne sont que deux. Pour réaliser leurs transactions hors-chaîne, ils ne recourent à aucun service autre que le réseau internet. Et le montant de leurs échanges n'a pour limite que leur apport initial en bitcoins.

Troisièmement, quand ils souhaitent fermer ce compte et récupérer la part qui revient à chacun, ils publient sur le réseau Bitcoin une transaction dite « de fermeture » qui est la dernière mise à jour des transactions réalisées entre eux deux sur ce canal. C'est le dernier état de leur compte mutuel, le solde de leurs échanges successifs. Le fait que ce soit la *dernière* mise à jour de la transaction en attente qui devienne normalement la transaction de fermeture est important pour le mécanisme anti-triche prévu dans ce dispositif *(cf. infra).*

Cette fermeture du canal peut être décidée à tout moment par l'une ou l'autre des deux parties. Il s'agit d'une transaction « normale » sur Bitcoin : elle est diffusée sur le réseau, validée par l'ensemble des nœuds, incluse dans un bloc et ainsi définitivement enregistrée dans la blockchain.

En résumé, **quel que soit le nombre d'échanges en bitcoins réalisés entre les deux participants, seules deux transactions auront**

été réalisées on-chain et seront donc inscrites définitivement dans la blockchain : la transaction d'ouverture du canal et celle de fermeture.

De cette manière, comme le dit Elizabeth Stark (CEO de la startup Lightning Labs), Lightning permet un *« consensus local » garanti en fin de compte par le consensus mondial (Bitcoin) ».* Un accord entre deux personnes sur le solde de leurs échanges est vérifié et scellé par le dispositif global et décentralisé de Bitcoin.

C) Mise en réseau des canaux de paiements

Il ne serait pas optimal de créer un canal de paiement avec chaque destinataire potentiel, notamment parce que cela nécessiterait autant de transactions *on-chain* que de destinataires. D'où l'idée de mise en réseau des canaux : **Lightning permet des paiements entre deux parties qui n'ont pas de canal de paiement direct entre elles mais qui en ont ouvert avec d'autres acteurs que l'on peut interconnecter.**

Les fonds circulent d'un utilisateur à l'autre, en empruntant le réseau formé par les canaux disponibles. La seule condition est qu'il existe au moins un chemin pour qu'ils parviennent à destination : il faut une succession de canaux de paiements ouverts par plusieurs personnes entre le payeur et le receveur.

Chacun peut décider d'être un nœud Lightning pour pouvoir ouvrir des canaux de paiements. Certains utilisateurs créent plusieurs canaux et se font connaître du réseau (grâce à une fonctionnalité automatique), pour servir d'intermédiaires, de relais : on les appelle « nœuds de routage » *(routing nodes)*. Ils peuvent le faire pour pouvoir être mieux connectés au réseau et réaliser des transactions plus facilement. Ils peuvent aussi, s'ils le souhaitent, prélever des frais sur les transactions qu'ils transmettent (le calcul de ces frais est très différent de Bitcoin et devrait, contrairement à lui, favoriser les micropaiements - *cf. infra*). Mais, comme pour les nœuds du réseau Bitcoin, cette fonction d'intermédiation ne leur confère aucun pouvoir de contrôle sur les fonds transmis.

Des acteurs comme les commerces recevant beaucoup de paiements pourront avoir intérêt à être bien connectés au réseau en ouvrant des canaux et des nœuds de routage, pour faciliter l'envoi de paiements vers leur adresse.

En revanche, certains nœuds ne peuvent pas relayer des transactions (comme les *wallets* pour mobiles, qui ne sont pas toujours connectés

au réseau) ou ne souhaitent pas le faire. Ces nœuds « périphériques» sont en bordure de la topographie du réseau. Ce sont des nœuds isolés, reliés par un seul canal de paiement à des nœuds plus connectés.

Si les nœuds ouvrant des canaux entre eux sont très nombreux, cela augmente la probabilité de trouver un chemin pour chaque transaction. Et cela augmente aussi les combinaisons possibles de canaux intermédiaires pour constituer cet itinéraire. C'est donc une évolution positive : plus le réseau Lightning abrite de canaux ouverts, plus il peut assurer sa fonction de réseau de paiement de manière efficace.

Un facteur favorise justement l'augmentation du nombre de canaux : **les utilisateurs ne sont jamais obligés de fermer leurs canaux.** Ils peuvent très bien décider d'en garder certains ouverts indéfiniment. Ils ont même intérêt à ne pas en fermer trop souvent, car chaque transaction de fermeture implique des frais de transaction sur le réseau Bitcoin.

On constate d'ailleurs que l'âge moyen des canaux identifiés augmente, ce qui montre qu'ils tendent à rester ouverts de plus en plus longtemps. C'est une bonne nouvelle. Et c'est très différent d'une situation où chaque utilisateur devrait ouvrir un canal avec chacun des autres, qui, elle, ne serait pas optimale *(cf. supra)*.

D) Contraintes pratiques

Pour utiliser Lightning, il faut, au préalable, posséder un *wallet* Lightning spécifique et l'avoir alimenté en bitcoins par une transaction *on-chain* normale. Par la suite, pour effectuer d'autres dépenses, il faut réalimenter régulièrement son *wallet,* comme on ajoute des pièces dans son porte-monnaie avant d'aller faire des courses. Par ailleurs, des projets sont en cours pour faciliter la réalimentation des canaux par des transferts directs depuis la blockchain Bitcoin. Ces opérations, à l'origine peu aisées pour le néophyte, sont maintenant plus accessibles. L'expérience utilisateur est en amélioration très rapide.

Une contrainte non négligeable est que, **contrairement à une transaction *on-chain,* il est nécessaire d'être connecté au réseau pour recevoir un paiement,** en raison du mécanisme de sécurisation des transactions prévu par le protocole *(cf. infra)*. C'est une différence par rapport à Bitcoin, où l'on peut recevoir une transaction sans être connecté. Très commentée lors du lancement de Lightning, cette contrainte ne semble pas si pénalisante dans la

pratique.

Par ailleurs, contrairement à Bitcoin, il est nécessaire de produire une nouvelle adresse pour chaque réception de paiement ; elle n'est pas réutilisable et a une durée de validité limitée à quelques heures.

Enfin, l'utilisateur doit aussi sauvegarder les informations contenues dans ses canaux, pour pouvoir récupérer ses fonds en cas de problème, notamment si le canal est fermé sans son accord *(cf. infra).* Cette opération est automatisée par la plupart des *wallets.*

E) Routage

Chaque émetteur de paiement décide des intermédiaires par lesquels il veut faire transiter ses fonds. A lui de trouver un chemin pour sa transaction. Cette opération, que l'on appelle « routage » est effectuée automatiquement. C'est l'une des fonctions des wallets.

Trouver un parcours qui optimise les frais payés aux intermédiaires est un enjeu important dans le fonctionnement du Lightning. Pour assurer cette tâche efficacement, l'algorithme de routage de chaque utilisateur doit être capable de recevoir et de traiter rapidement une masse d'informations considérable : topographie du réseau, capacité des canaux, niveau des frais de routage, etc.

D'intenses efforts scientifiques sont consacrés au maintien d'un routage efficace à long terme. Il s'agit d'un défi mathématique et informatique notable. Alors que Bitcoin agençait (d'une manière certes exceptionnellement novatrice) des technologies éprouvées depuis des années (cryptographie asymétrique, registres distribués, preuve de travail, *peer-to-peer*, etc.), le développement de Lightning nécessite parfois de résoudre des problèmes nouveaux, surtout en matière de routage.

Plusieurs chercheurs de haut niveau s'y sont attelés avec succès. De nombreuses pistes d'amélioration sont à l'étude ou en cours de développement. Par exemple, un projet d'optimisation appelé « Trampoline » permet de déléguer une partie des calculs de routage à un tiers sans sacrifier le niveau de confidentialité. On peut aussi citer la proposition d'algorithme d'ant routing (en référence aux méthodes sophistiquées de recherche de nourriture des fourmis) des mathématiciens Ricardo Pérez-Marco (CNRS, Université Paris XIII) et Cyril Grunspan (Ecole supérieure d'ingénieurs Léonard de Vinci – Esilv).

F) Centralisation

Un des premiers risques soulignés lors du lancement du Réseau Lightning a été celui d'une centralisation du réseau autour de quelques nœuds de routage importants. Dans ce scenario, quelques nœuds de routage, capables d'ouvrir énormément de canaux de paiements et d'y maintenir beaucoup de liquidité *(cf. infra)*, deviendraient incontournables dans les chemins utilisés pour les transactions. Cette situation irait à l'encontre de l'objectif de décentralisation du réseau. Elle conférerait à ces nœuds un pouvoir de surveillance et de censure *(cf. infra)*. Elle leur donnerait la possibilité d'imposer des frais excessifs. Et elle pourrait également fragiliser techniquement le réseau, à travers des défaillances éventuelles de canaux de paiement massifs.

Une telle évolution constituerait un retour en arrière quelque peu ironique puisque l'intérêt principal de Lightning est d'assurer la scalabilité de Bitcoin sans prendre le risque de centralisation du réseau qu'aurait impliquée l'autre option envisagée, celle de l'augmentation rapide de la taille des blocs.

Pour rappel, sur Bitcoin, des blocs beaucoup plus gros nécessiteraient davantage de moyens pour les *full-nodes* (qui sont bénévoles s'ils ne font pas de minage) comme pour les mineurs : cela réduirait leur nombre et compliquerait aussi le processus de propagation à tout instant du dernier bloc à l'ensemble du réseau, remettant ainsi en question l'un des principaux mécanismes de sécurisation de Bitcoin. Cet aspect est crucial : Lightning est un dispositif certes beaucoup plus complexe qu'une simple augmentation de la taille des blocs, mais qui permet de ne pas compromettre la sécurité du système (par ailleurs, notons que la taille des blocs pourrait augmenter à l'avenir, avec des effets de scalabilité démultipliés par le *layer 2*).

S'agissant du réseau Lightning, si des nœuds de routage acquièrent un poids majeur, il faut qu'ils puissent être contournés facilement, pour réduire les inconvénients de la centralisation. La priorité est donc qu'il reste techniquement possible de faire tourner des nœuds permettant ce contournement si nécessaire.

Or, **les barrières à l'entrée techniques et financières pour constituer un nœud relai Lightning sont faibles,** notamment si on les compare aux investissements nécessaires pour miner sur Bitcoin. N'importe qui peut le faire pour un coût négligeable. Il convient juste de posséder un nœud complet Bitcoin, ce qui n'est pas encore très répandu mais devient de plus en plus facile. Cela reste à confirmer, et des débats demeurent sur ce sujet, mais on peut imaginer que

cette caractéristique permette à l'avenir de maintenir naturellement un niveau de décentralisation satisfaisant sur le réseau Lightning.

G) Liquidité

Un autre défi du réseau Lightning est la question de la disponibilité des fonds sur chaque canal. Pour faire transiter des fonds entre divers canaux de paiements, il faut qu'une somme équivalente soit déjà contenue dans chacun d'eux.

C'est l'un des aspects les moins intuitifs de Lightning. Les canaux de sont pas une sorte de « tuyaux » vides dans lesquels on fait passer de l'argent : ils représentent plutôt des segments contractuels entre plusieurs acteurs, dans lesquels la répartition de la propriété des bitcoins est modifiée à chaque transaction, pour faire circuler des fonds d'un point à un autre. Dans un canal de paiement Lightning, la somme totale de bitcoins ne varie pas : c'est uniquement leur répartition entre les deux parties qui est modifiée successivement entre eux, même quand ce canal est utilisé par un nœud de routage pour transmettre une transaction.

La nécessité de maintenir une liquidité suffisante pour que les fonds puissent circuler d'un canal à l'autre peut d'ailleurs fournir une incitation financière pour les nœuds de routage ou d'autres acteurs à offrir de la liquidité pour attirer les transactions et percevoir des frais *(cf. infra)*.

Par ailleurs, de nouvelles fonctionnalités sont à l'étude, par exemple celle consistant à fractionner entre plusieurs itinéraires une transaction de montant élevé qui ne pourrait pas trouver de canaux disposant de suffisamment de liquidités par lesquels transiter : les Atomic Multipath Payments (AMP).

H) Mécanisme anti-triche

Faire fonctionner un dispositif comme Lightning en limitant les risques de fraude, de détournement et de vol est un défi technique d'une grande complexité, et les nombreux niveaux de cryptographie déployés pour y répondre sont impossibles à résumer ici.

Le cas le plus emblématique est celui d'une tentative de vol par un des deux titulaires d'un canal (ce peut être un nœud de routage censé relayer la transaction). Par définition, les bitcoins placés dans un canal de paiement sont bloqués en dehors de la blockchain. Cela

signifie que, tant que leur répartition entre les deux utilisateurs n'a pas été « scellée » définitivement par une transaction consensuelle *on-chain*, **chacun peut tenter de spolier l'autre en effectuant une fermeture unilatérale du canal qui ne publierait pas sur la blockchain le solde final de leurs échanges mais un état antérieur qui lui serait plus favorable.** Autrement dit, pour voler des bitcoins sur Lightning, il est possible d'essayer de publier une transaction de son canal qui n'est pas la dernière en vigueur.

Ce risque aurait bien sûr rendu impossible tout essor du réseau Lightning si un mécanisme ingénieux n'avait été imaginé pour le surmonter : la partie spoliée qui repère la transaction *on-chain* frauduleuse dispose d'un délai (de quelques jours, et pouvant être paramétré) pour l'annuler et récupérer l'ensemble des fonds du canal. Pour pouvoir détecter ce type de tentative, les utilisateurs du réseau Lightning doivent surveiller la blockchain régulièrement ; dans la pratique, cette tâche est automatisée ou externalisée à peu de frais à des prestataires spécialisés.

L'utilisateur spolié récupère non seulement sa part légitime mais aussi celle du tricheur. **Ce mécanisme est donc particulièrement dissuasif** : d'une part, le voleur a très peu de chances de réussir son coup ; d'autre part, s'il échoue il est certain de perde ses propres fonds.

Notons que ce mécanisme ne remet pas pour autant en question le principe d'irréversibilité de la transaction, l'un des piliers de Bitcoin. Il ne peut normalement être actionné que si l'un des utilisateurs a vraiment tenté de voler l'autre (des recherches sont toutefois en cours pour l'affiner en cas de fermeture accidentelle de canal sans intention frauduleuse).

A l'instar de Bitcoin et de son dispositif de minage, ce protocole peut ainsi s'analyser en théorie des jeux comme un **ensemble d'incitations qui rendent plus rationnel économiquement de contribuer à sécuriser le réseau plutôt que d'essayer de le pirater.** Comme Bitcoin, Lightning permet des paiements entre des interlocuteurs qui n'ont aucune raison de se faire confiance, en utilisant un réseau pair-à-pair composé d'acteurs à qui il n'est nul besoin de faire confiance.

I) Confidentialité

Lightning offre un niveau de confidentialité supérieur à Bitcoin, essentiellement parce qu'il ne repose pas sur un registre public : seules les transactions d'ouverture et de fermeture de canaux sont publiques, enregistrées et traçables.

Il convient d'ailleurs de remarquer que cette confidentialité supérieure est obtenue au prix d'un niveau de sécurité un peu inférieur à celui du réseau *on-chain*. L'arbitrage confidentialité/sécurité n'est pas le même entre Lightning et Bitcoin. Il est impossible de maximiser tous les paramètres en même temps. Ce qui compte, c'est que les arbitrages soient explicités et assumés, ce qui est loin d'être toujours le cas dans l'univers des cryptomonnaies.

Comme le registre n'est pas public, les transactions *off-chain* pourraient, en revanche, être observées par les nœuds intermédiaires. Ce risque serait d'autant plus préoccupant si la centralisation du réseau augmentait *(cf. supra)* : si quelques nœuds de routage importants centralisaient l'essentiel des flux, cela augmenterait leurs possibilités de surveillance ou de censure. Comme pour Bitcoin, il est donc préférable que le réseau soit aussi décentralisé que possible, avec un maximum de nœuds et de canaux.

Afin de limiter tout risque de surveillance, les entreprises développant le réseau se sont mises d'accord pour utiliser la technique de l'onion routing (comme le réseau Tor). Le chiffrement cryptographique du paiement est effectué d'une manière telle que chaque intermédiaire n'a accès qu'à l'information qui le concerne : d'où vient le paiement, quel montant il doit transmettre, et à quelle adresse. Les couches de chiffrement s'épluchent comme les feuilles d'un oignon. Impossible pour un nœud de routage de savoir par combien d'autres intermédiaires passera le paiement, ni à quel stade il se trouve lui-même dans son parcours.

Enfin, comme pour les nœuds Bitcoin, l'utilisation de Tor pour éviter de révéler son adresse IP est conseillée. Certes, de nouvelles techniques de surveillance seront sans doute déployées mais on peut imaginer que les techniques de protection se développeront en parallèle, comme c'est déjà le cas pour Bitcoin. Pour l'heure, le réseau Lightning semble robuste.

Finalement, **sur Lightning comme sur Bitcoin, les paiements circulent par des intermédiaires mais ceux-ci ne sont pas des tiers de confiance** : le système ne leur concède ni l'information pertinente ni l'incitation économique, ni la possibilité technique pour tenter de censurer ces paiements.

Cette caractéristique est totalement nouvelle par rapport aux systèmes de paiements traditionnels reposant notamment sur les réseaux bancaires. Sur ces derniers, les « tiers de confiance » agréés ont la possibilité de tout connaître de chaque transaction et d'interrompre celles de leur choix pour tout motif (réglementations, pressions politiques, corruption, etc.). Par ailleurs, étant centralisés, ils sont techniquement vulnérables et représentent des cibles contre lesquelles il est rationnel économiquement pour certains acteurs d'investir de forts moyens de piratage. Comme le résume Nick Szabo (l'un des principaux inspirateurs de Bitcoin) "trusted third parties are security holes".

III - Eléments financiers

A) Régime des frais de routage

Comme sur Bitcoin, les frais assumés par le payeur constituent une incitation financière rémunérant les acteurs qui font fonctionner le réseau : les mineurs, dans le cas de Bitcoin, et les nœuds de routage, pour Lightning. Mais deux aspects distinguent Lightning et Bitcoin.

D'une part, le payeur ne détermine pas les frais qu'il souhaite payer de la même manière que sur Bitcoin. Sur Bitcoin, il les choisit essentiellement en fonction de la vitesse de validation qu'il désire (les mineurs sélectionnant les transactions à traiter en priorité en fonction de ces frais). **Sur Lightning, les nœuds de routage choisissent et annoncent le niveau des frais qu'ils souhaitent prélever, et l'algorithme de routage du payeur décide des nœuds par lesquels faire passer les fonds,** notamment en fonction de ces frais. Les algorithmes des *wallets* effectuent des tentatives incrémentales en faisant varier le niveau possible de frais, jusqu'à trouver un chemin optimal.

L'utilisateur peut ainsi choisir les nœuds qui proposent les frais les plus faibles. Il peut aussi consentir des frais plus élevés, si c'est le prix à payer pour passer par davantage d'intermédiaires et ainsi renforcer la confidentialité de la transaction. Enfin, si les frais demandés par les nœuds relais sont trop élevés, l'algorithme de routage peut renoncer à trouver un chemin, et abandonner la transaction.

D'autre part, **sur Lightning, ces frais ne sont pas calculés par rapport à la quantité d'information utilisée pour chaque transaction et circulant sur le réseau mais essentiellement en proportion du montant de la transaction** (outre ces frais exprimés en pourcentage, s'ajoute une petite part forfaitaire, dite « frais de base », exprimée en satoshis).

Cette différence de calcul des frais provient du fait que sur Bitcoin et Lightning, ce n'est pas l'usage de la même ressource rare qui est rémunéré : sur le *layer 1*, c'est la taille des blocs et la capacité de stockage de la blockchain (qui contraignent le volume d'information que l'on peut diffuser sur le réseau et impose d'organiser un ordre de priorité pour les transactions à miner) ; sur le *layer 2*, c'est la liquidité des canaux (qui contraint les montants que l'on peut faire circuler sur le réseau).

Ces différences dans la fixation des frais entraînent des conséquences dans deux domaines : en matière de services de paiement et d'activité financière.

B) Micro paiements et monnaie en streaming

Le fait que les frais de routage soient proportionnels aux sommes échangées rend rentables économiquement des transactions de très faible montant, et même des micropaiements, par exemple de l'ordre du satoshi – et moins encore. C'est impossible dans les systèmes de paiements traditionnels à cause du coût de l'intermédiation nécessaire à la sécurisation des réseaux. Et c'est économiquement rédhibitoire sur Bitcoin, où les frais de transaction incompressibles sont plus élevés que le niveau de ces micro-transactions.

A l'avenir – surtout si les frais de transaction progressent sur Bitcoin – il est prévisible que les montants faibles et les micropaiements se feront exclusivement sur le réseau Lightning, tandis que les transactions de montants plus significatifs se feront *on-chain*, où il sera rationnel de consentir des frais plus élevés pour profiter de la sécurité maximale de la blockchain.

Par ailleurs, les micropaiements permis par Lightning ouvrent des possibilités techniques insoupçonnées, au-delà du seul paiement : ils peuvent, par exemple, être utilisés pour rendre à la fois plus fiables, plus simples et plus confidentiels les processus d'authentification sur internet (*logins*, mots de passe, etc.), grâce au projet de Lightning Service Authentication Tokens (LSATs).

Lightning pourrait s'avérer utile pour moderniser le commerce de détail. Avec ce protocole, c'est le consommateur qui assume les frais de transaction, alors qu'avec les réseaux de paiements par carte (Visa, Mastercard, etc.)., ce sont les commerçants qui assument les frais. Ces derniers sont répercutés dans les prix de vente et pèsent donc *in fine* sur le consommateur final, mais le système du Lightning est plus simple et plus transparent. Surtout, il permet d'éviter la fraude liée au paiement par carte bancaire, qui représente un coût considérable au niveau mondial.

S'agissant des flux spéculatifs, qui représentent encore l'essentiel des paiements en bitcoins, il semble qu'ils n'aient pas actuellement besoin d'une surcouche comme Lightning. D'autant plus qu'ils disposent maintenant d'une autre option pour effectuer des transactions plus rapides que sur la simple blockchain : le réseau Liquid (mis en place en 2018 par la société Blockstream), qui n'est pas un layer 2 mais une sidechain de Bitcoin.

Enfin, en combinant cette possibilité de micro-transactions avec le caractère pratiquement instantané des paiements (pas besoin d'attendre l'enregistrement du bloc dans la blockchain), **il devient possible de réaliser des paiements en flux, des cash flows au sens propre du terme**, de la « monnaie en streaming », selon l'expression d'Andreas Antonopoulos.

Les applications financières et industrielles de cette avancée sont illimitées : payer automatiquement son électricité à la milliseconde, toucher son salaire en temps réel au lieu d'une fois par mois, facturer des services en streaming, monétiser les flux de données (personnelles) sur internet, etc. Elles seront, par ailleurs, décuplées par leur intégration aux relations de machine à machine, aux objets connectés.

Tous ces éléments cumulés permis par Lightning – micropaiement, intérêt pour les commerçants, monnaie en streaming et paiements de machine à machine – laissent entrevoir une potentielle révolution historique du paiement.

C) Economie financière

Ouvrir un nœud de routage et alimenter des canaux de paiement pour toucher des frais de transaction pourrait bien devenir une activité commerciale à part entière.

L'existence d'une rémunération pour la transmission des transactions est d'ailleurs une différence importante entre Lightning et le réseau

Tor. Ce dernier a probablement pâti de l'absence d'incitation financière offerte aux acteurs qui contribuent à construire le réseau. La monétisation des nœuds du réseau Lightning est un mécanisme vertueux qui joue théoriquement en faveur de son développement.

Pour attirer des transactions et collecter des frais, les opérateurs de nœuds de routage doivent s'assurer que leurs canaux de paiement conservent une certaine quantité de bitcoins (*cf. supra*) : il leur faut à la fois une capacité « entrante » et une « sortante », pour respectivement recevoir et transmettre des fonds (c'est vrai également pour des nœuds qui effectueraient beaucoup d'opérations sur le réseau sans nécessairement chercher à être des nœuds de routage).

Cet impératif de maintien d'une certaine liquidité sur le réseau implique une gestion active des fonds en bitcoins entre canaux par les opérateurs de nœuds de routage. Elle suscite des stratégies et méthodes d'allocation de plus en plus sophistiquées, avec notamment l'apparition de nouveaux acteurs, les « fournisseurs de liquidités » (par exemple Bitrefill ou LNBig).

Opérer un nœud de routage et/ou fournir des liquidités représente ainsi un réel investissement en travail et en capital. C'est non seulement le seul moyen de « prêter » (sans toutefois qu'il y ait un « emprunteur » pouvant en disposer) des bitcoins sans se séparer de ses clés privées ; c'est aussi une manière de placer du capital de manière relativement peu risquée et de toucher une rémunération pouvant éventuellement devenir plus attrayante que sur les marchés financiers classiques, surtout dans un contexte de taux d'intérêt négatifs.

Aujourd'hui, le routage est encore peu rentable. Certains intermédiaires fixent d'ailleurs des frais nuls pour développer le réseau. Mais si Lightning se développe, ces nouveaux business pourraient devenir lucratifs, même si la concurrence entre les nœuds tend à égaliser à la baisse le niveau moyen des frais (une différenciation des services et des prix pouvant toutefois rester possible).

Enfin, la rémunération moyenne servie sur Lightning pourrait un jour fournir la meilleure approximation de ce que serait le taux d'intérêt naturel du marché sans risque, non faussé par les réglementations des Etats et les politiques monétaires des banques centrales (plus précisément, il s'agirait d'un risque différent : non pas un risque de contrepartie mais un risque technique de piratage nécessitant des investissements en sécurité). Elle pourrait même aboutir, comme l'a suggéré le financier Nik Bhatia, à un taux de référence de l'économie Bitcoin, tout comme il existe plusieurs taux de référence pour le dollar.

Conclusion

Comme Internet, Lightning est un empilement de technologies complexes et au potentiel immense. Il répond à un besoin qui a été identifié dès les débuts de Bitcoin : effectuer des transactions en bitcoins instantanées et anonymes, des micropaiements pour des frais négligeables, un passage à l'échelle sans dépense énergétique additionnelle.

L'infrastructure du réseau Lightning n'est pas achevée. D'intenses efforts techniques et scientifiques sont actuellement fournis pour la perfectionner. Mais les progrès récents et en cours s'accumulent à une vitesse impressionnante (on parle d'ailleurs déjà de *layer 3* se superposant au *layer 2*, par exemple le protocole RGB).

Lightning a probablement le potentiel de révolutionner l'industrie du paiement et une partie du secteur financier, et d'accélérer massivement la diffusion de Bitcoin comme système monétaire alternatif. C'est ce que l'on peut imaginer si le rythme de son développement se poursuit. Or (comme le suggèrent notamment les récentes levées de fonds de deux des entreprises qui y contribuent, Acinq et Lightning Labs), il n'y a, à ce stade, pas de raison que ce rythme ralentisse.