Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Communication FINMA sur la surveillance 08/2023

Staking

20 décembre 2023

Laupenstrasse 27, 3003 Berne, tél. +41 (0)31 327 91 00, www.finma.ch

Table des matières

1 Introduction

Une base légale relative à la conservation des cryptoactifs a notamment été créée avec l'entrée en vigueur du projet TRD. Elle protège les clients en cas d'insolvabilité du dépositaire. En raison de l'importance croissante des services dits de *staking*, la FINMA a dû répondre à des questions de plus en plus nombreuses concernant l'application de ces dispositions en matière de conservation aux offres de *staking*. Selon les modalités du service de *staking*, les exigences du projet TRD pourraient éventuellement ne pas être satisfaites et les actifs pourraient ne pas être protégés contre l'insolvabilité en cas d'insolvabilité du dépositaire.

Les questions évoquées ont pris de l'importance notamment suite à la transition de la *blockchain* Ethereum vers le mécanisme de la preuve d'enjeu *(proof of stake)*, à l'évolution de la situation macroéconomique et à l'adaptation des taux d'intérêt, ce qui accentue la nécessité d'agir. La FINMA a discuté de ce sujet avec des représentants de la branche dans le cadre de tables rondes afin de sensibiliser les acteurs du marché concernés à la thématique du *staking*. Une enquête a par ailleurs été organisée auprès de différents établissements assujettis au sujet de leurs services de *staking*.

Par la présente communication sur la surveillance, la FINMA rend compte du résultat de la discussion sur la classification des prestations de *staking* selon le droit des marchés financiers. Il s'agit notamment de préciser l'interprétation des lois concernant la distinction entre valeurs déposées protégées en cas de faillite et dépôts exposés au risque d'insolvabilité, les obligations correspondantes en matière d'autorisation selon le droit bancaire ainsi que les conséquences sur les exigences en matière de fonds propres des établissements autorisés.

2 *Staking*

2.1 Description

Il n'existe pas pour l'instant de définition uniforme du terme *« staking »*. Par *staking*, la FINMA entend le processus de blocage des cryptoactifs natifs à l'adresse de *staking* d'un nœud de validation afin de participer au processus de validation d'une *blockchain* fondée sur le mécanisme de consensus de la preuve d'enjeu. Les participants reçoivent des *staking rewards* en récompense du *staking* de cryptoactifs.

Les *blockchains* fondées sur la preuve d'enjeu se distinguent entre elles, dans le sens que le processus inverse de l'*unstaking* inclut parfois une pé-

riode de blocage/sortie (variable), qui retarde le retrait des cryptoactifs bloqués. De plus, les *blockchains* génèrent aussi parfois des incitations négatives pour une activité de validation conforme aux règles. En règle générale, les cryptoactifs bloqués pour le *staking* peuvent ainsi être soumis à une radiation *(slashing)* partielle ou complète en cas de problème au niveau d'un nœud de validation.

2.2 Variantes

Différentes variantes du *staking* ont vu le jour en pratique. Aux fins de la présente communication sur la surveillance, nous distinguons les situations suivantes :

- ***Custodial staking*** : dans le cas du *custodial staking*, le client transfère les cryptoactifs à un prestataire. Le *custodial staking* inclut également les deux variantes du *direct staking* et de la chaîne de *staking* :
  - ***Direct staking*** : dans le cas du *direct staking*, le prestataire exploite lui-même le nœud de validation ou en externalise l'exploitation à un prestataire technique, mais conserve au moins lui-même les clés de retrait *(withdrawal keys)* permettant de retirer les cryptoactifs stakés du client.
  - **Chaîne de *staking*** : dans une chaîne de *staking*, les cryptoactifs à staker sont transmis par le prestataire entretenant la relation client à un ou plusieurs tiers qui exploitent le nœud de validation et qui disposent des clés de retrait.
- ***Non-custodial staking* :** dans le *non-custodial staking*, les clients conservent le contrôle exclusif des clés de retrait, raison pour laquelle il n'y a pas non plus de conservation ni d'acceptation d'actifs par des tiers.

2.3 Risques

Le recours aux services de *staking* recèle différents risques :

- Risque technique de dysfonctionnement du processus de *staking* ; il existe en outre un risque de *slashing* des cryptoactifs suite à un comportement problématique du nœud de validation ; les sanctions peuvent aussi être automatiques lorsque le nœud de validation est par ex. hors ligne suite à des problèmes techniques ou faute de mesures de gestion de la continuité des affaires suffisantes.
- Risque de contrepartie dû à une situation juridique incertaine en cas de faillite ; il existe actuellement en Suisse une incertitude juridique concernant le traitement des cryptoactifs stakés en droit de la faillite dans certains cas de figure (voir le chapitre 3.2). Cette incertitude juridique est d'autant plus forte lorsque la conservation ou le *staking* sont délégués à des établissements étrangers, car le traitement des cryptoactifs selon le

droit de la faillite n'est souvent pas spécifiquement réglementé à l'étranger.

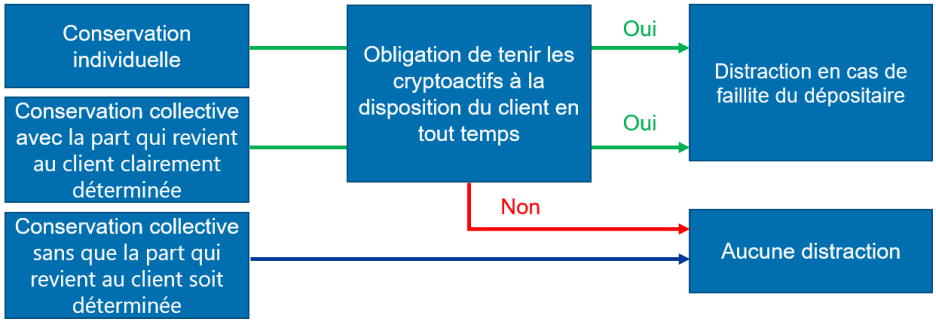
- Risque de marché, car les cryptoactifs *stakés* ne peuvent éventuellement pas être vendus au bon moment dans une période de volatilité, lorsque le processus d'*unstaking* inclut une période de blocage/sortie, qui retarde le retrait des cryptoactifs bloqués. Dans certaines *blockchains* comme Ethereum, la période de blocage est plus longue, lorsque le nombre d'ordres d'*unstaking* augmente, ce qui peut se traduire par des périodes de blocage très longues en période de crise et par une impossibilité technique passagère de vendre les cryptoactifs. La durée de la période de blocage est parfois imprévisible et opaque pour les clients, compte tenu de l'évolution constante de la *withdrawal-queue* et du nombre de validateurs.

3 Traitement réglementaire

3.1 Bases de la conservation des cryptoactifs

Le projet TRD est intégralement entré en vigueur le 1er août 2021. Le nouvel art. 242*a* LP a créé une base légale pour la conservation des cryptoactifs à l'abri de la faillite. Le graphique suivant présente les conditions requises pour une distraction en cas de faillite du dépositaire.

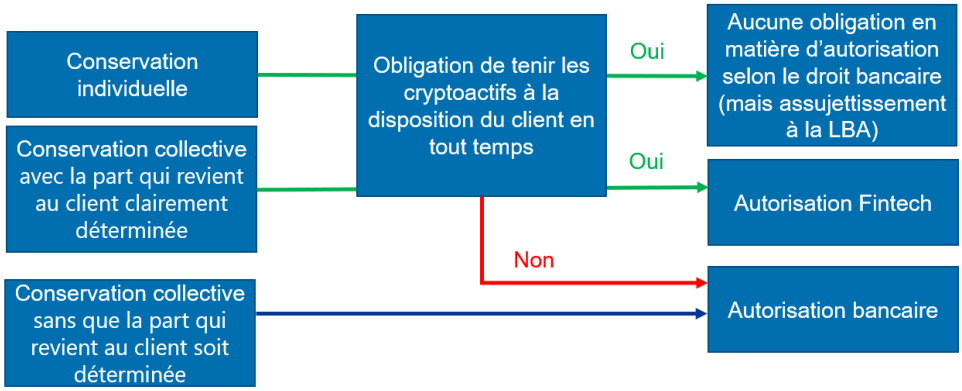
Traitement en droit de la faillite (art. 242*a* al. 2 LP) :



Dans le cadre du projet TRD et en conformité avec cette réglementation du droit de la faillite, une disposition équivalente a également été insérée à l'art. 16 ch. 1bis LB pour les établissements régis par le droit bancaire. L'art. 16 LB décrit les valeurs déposées qui, en cas de faillite, sont distraites de la masse au bénéfice des clients déposants conformément à l'art. 37*d* LB. La distraction vise un traitement privilégié des valeurs qui figurent sur le relevé de dépôt des clients déposants et qui ne sont pas tenues dans les livres de la banque.

Ces dispositions sont également importantes pour l'évaluation des éventuelles obligations en matière d'autorisation selon le droit bancaire. Outre l'acceptation à titre professionnel de dépôts du public, l'acceptation à titre professionnel de moyens de paiement cryptographiques en dépôt collectif (jetons de paiement) au sens de l'art. 5*a* OB est aussi explicitement soumise à autorisation, depuis l'entrée en vigueur du projet TRD.

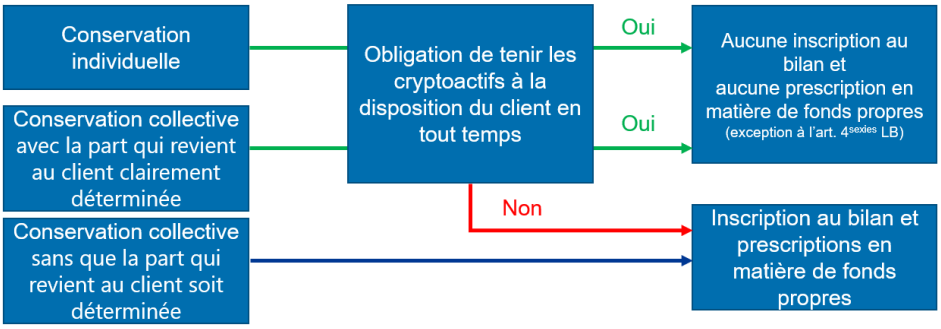
Traitement en droit bancaire (art. 1*a* et 1*b* LB en relation avec les art. 5 et 5*a* OB) :



La conservation des jetons de paiement sur un compte collectif , avec la part qui revient au client clairement déterminée, requiert une autorisation selon le droit bancaire. Une autorisation Fintech selon l'art. 1*b* LB est suffisante pour ce type de garde, pour autant que les jetons de paiement soient disponibles en tout temps. En revanche, la conservation individuelle de jetons de paiement tenus à disposition du client en tout temps ne requiert pas d'autorisation bancaire. De tels dépositaires sont toutefois considérés comme des intermédiaires financiers soumis à la LBA, qui doivent s'affilier à un organisme d'autorégulation pour la surveillance en matière de blanchiment d'argent.

Dans le cas des banques, la question qui se pose en outre est de savoir quels cryptoactifs conservés doivent être inscrits au bilan en tant que dépôts et lesquels peuvent être tenus comme valeurs déposées en dehors du bilan. Cette question est importante, car des exigences prudentielles doivent être satisfaites pour les actifs inscrits au bilan.

Enregistrement comptable et exigences prudentielles :



La qualification en tant que valeurs déposées hors bilan suppose nécessairement que les cryptoactifs soient *en tout temps tenus à la disposition du client*. Lorsque les cryptoactifs ne sont pas en tout temps tenus à la disposition du client, il s'agit dans le cas des jetons de paiement de dépôts du public devant être portés au bilan, ce qui déclenche des exigences supplémentaires en matière de fonds propres. Dans le cas de cryptoactifs en dépôt collectif, la qualification en tant que valeur déposée requiert en outre que les parts des clients déposants dans la fortune collective soit clairement déterminée (par ex. grâce à un registre interne qui attribue clairement les cryptoactifs aux clients respectifs et qui permet de les distraire en leur faveur en cas de faillite).

3.2 Applicabilité au *staking*

Différentes questions d'interprétation des dispositions en matière de conservation présentées se posent en lien avec les services de *staking*. Elles concernent principalement la condition essentielle pour la protection en cas de faillite selon laquelle les cryptoactifs doivent en tout temps être tenus à la disposition des clients.

Cette condition n'est pas remplie lorsque le dépositaire pratique le *staking* pour propre compte. Dans de telles situations, il faut considérer qu'il s'agit d'une opération pour compte propre au sens de l'art. 1*a* let. b LB. Par conséquent, de tels cryptoactifs stakés pour le propre compte du dépositaire ne peuvent pas être séparés ou distraits en cas de faillite et sont soumis aux exigences en matière de fonds propres.

La situation juridique est incertaine lorsque le *staking* est pratiqué au nom et pour le compte des clients. Dans de telles situations, le mécanisme de *staking* concret de la *blockchain* concernée doit être apprécié au cas par cas.

Les *blockchains* qui ne prévoient ni période de blocage ni mécanisme de sanction *(slashing)* pour le *staking* semblent en principe ne pas poser de problème dans la perspective de la protection contre la faillite. En l'absence

de périodes de blocage, de *slashing* ou de restrictions comparables du droit de libre disposition, les cryptoactifs sont en tout temps tenus à la disposition du client et peuvent donc généralement aussi être séparés ou distraits.

Le message relatif au nouvel art. 242*a* LP retient : « cela signifie concrètement que, dès le moment où le tiers lui a cédé le pouvoir de disposer des biens ou dès le moment où il a acquis le pouvoir de disposer des biens pour le compte du tiers, le failli est tenu d'avoir le pouvoir de disposer des biens (au sens de l'al. 1) de manière ininterrompue. Il suffit cependant qu'il possède de manière ininterrompue le nombre d'unités détenues pour le tiers pour que l'obligation soit considérée comme remplie. Autrement dit, il est permis de remplacer certains jetons, pour autant que le nombre total de jetons ne soit jamais inférieur à la quantité requise pour pouvoir désintéresser l'ayant droit en tout temps. »[1]

Lorsque les cryptoactifs en dépôt sont exposés à un risque de *slashing* et/ou à un retard lors de l'*unstaking* (période de blocage/sortie) dans le cadre du service de *staking*, le prestataire conserve certes le pouvoir de disposition sur les clés de retrait, mais il n'est pas certain que l'on puisse considérer selon le message du Conseil fédéral que la restitution des cryptoactifs en dépôt à l'ayant droit puisse être garantie en tout temps. On peut donc se demander si la condition de la tenue à disposition en tout temps au sens de l'art. 242*a* al. 2 LP et de l'art. 16 ch. 1bis LB est remplie. Il s'agit là *de lege lata* d'une incertitude juridique.

L'exigence de la tenue à disposition en tout temps émane de la norme spéciale spécifique à la technologie de l'art. 242*a* al. 2 LP et de l'art. 16 ch. 1bis LB, qui a été définie par rapport à des questions en lien avec la conservation et non avec le *staking*, en raison de la situation à la date à laquelle le projet de loi a été rédigé. Il n'existe pas pour l'instant de jurisprudence pertinente ni de pratique des juges de la faillite permettant de savoir si les cryptoactifs stakés sur des *blockchains* avec des périodes de blocage et/ou un *slashing* remplissent encore l'élément constitutif de la tenue à disposition en tout temps. Les recommandations internationales concernant le traitement du *staking* font également défaut.

[1] Message du 27 novembre 2019 relatif à la loi fédérale sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués, FF **2020** 223, consultable sous : https://www.fedlex.admin.ch/eli/fga/2020/16/fr.

4 Conséquences juridiques

4.1 *Staking* par des établissements autorisés

4.1.1 Chaîne de *staking*

Lorsqu'un établissement délègue l'exploitation du nœud de validation à un tiers (autres banque ou exploitant d'un *pool* de *staking*) dans le cadre d'une chaîne de *staking*, il possède au plan comptable une créance envers cette partie contractante de l'établissement autorisé (ci-après qualifié de « prestataire tiers »). Cette créance peut être portée au bilan comme créance envers le prestataire tiers ou être traitée comme une créance en dépôt fiduciaire au sens de l'art. 16 ch. 2 LB et donc comme une valeur déposée, pour autant que certaines conditions soient respectées.

La possibilité de distraction visée à l'art. 16 ch. 2 LB suppose une application par analogie des directives de SwissBanking concernant les placements fiduciaires adaptée aux risques des cryptoactifs, afin d'exclure la négligence grave des dépositaires vis-à-vis de leurs clients. Cette précision est nécessaire afin de tenir compte des risques spécifiques du *staking*.

L'hypothèse d'une telle relation fiduciaire en lien avec le *staking* nécessiterait donc au minimum une convention fiduciaire avec un mandat fiduciaire spécifique du client ainsi que sa sélection des cryptoactifs et du montant, incluant une information complète sur les risques du client en relation avec le mandat de *staking* (notamment *slashing* et période de blocage) et conforme aux obligations restantes énoncées dans les directives.

L'établissement doit notamment :

- limiter les risques de contrepartie en choisissant un établissement soumis à une surveillance prudentielle affichant une bonne solvabilité ou la filiale d'un groupe financier consolidé soumis à une surveillance prudentielle affichant une bonne solvabilité ; et
- garantir au moyen d'une *due diligence* spécifique que :
  - le prestataire tiers n'exerce pas son activité sans droit ;
  - le prestataire tiers détient lui-même les clés de retrait déterminantes, ce qui exclut les chaînes de *staking* longues. Si le prestataire tiers souhaite recourir à un prestataire supplémentaire, il convient de vérifier au cas par cas que les mesures d'adaptation (par exemple un *pre-signing* de la transaction de retrait) ont un effet équivalent ;
  - le prestataire tiers désigne les adresses de validation (par ex. au moyen d'un registre interne) sur lesquelles il détient les cryptoactifs des dépositaires et les en informe ;

- le prestataire tiers a pris toutes les mesures nécessaires pour limiter les risques opérationnels concernant l'exploitation du nœud de validation (erreur de validation ou statut hors ligne), exclure des sanctions supplémentaires à l'encontre du validateur et assurer la continuité des affaires ; et
- en cas de recours à des prestataires étrangers, ceux-ci doivent être soumis à une surveillance prudentielle dans une juridiction à la réglementation équivalente, qui offre la même sécurité juridique que la Suisse concernant le traitement des cryptoactifs déposés en droit de la faillite, en plus des conditions précitées et faire l'objet d'une *due diligence* spécifique, qui inclut les points précités pour les prestataires suisses.

- établir un *digital assets resolution package* (DARP) aux fins d'une gestion des risques appropriée, qui est régulièrement mise à jour et :
  - qui contient les principales informations requises pour identifier et pour garantir immédiatement les cryptoactifs (par ex. description du type de conservation, informations sur les personnes de contact ayant accès aux clés privées, informations sur les tiers dépositaires, etc.) ;
  - qui garantit que le liquidateur pourra verser rapidement les cryptoactifs aux clients en cas de faillite, de manière à limiter au maximum les charges et les coûts requis pour une restitution en bonne et due forme.

4.1.2 Direct staking

En cas de *direct staking*, l'établissement pratique généralement lui-même le *staking* et a également le pouvoir de disposition sur les clés de retrait permettant de retirer les cryptoactifs bloqués. Une distraction par le biais de l'art. 16 ch. 2 LB n'est donc pas envisagée.

Comme évoqué précédemment au chapitre 3.2, il y a une incertitude juridique quant à savoir si la condition de la tenue à disposition en tout temps au sens de l'art. 242*a* al. 2 LP et de l'art. 16 ch. 1bis LB est remplie.

Eu égard à cette situation juridique incertaine, la FINMA renonce pour l'instant à exiger le respect des exigences en matière de fonds propres concernant les cryptoactifs stakés dans les banques, dans la mesure où (cumulativement) :

- il y a une instruction spécifique du client sur le type et la quantité de cryptoactifs à staker ;
- des mesures appropriées garantissent que les cryptoactifs placés sur une certaine adresse de validation et après l'*unstaking* sur une certaine adresse de retrait puissent toujours être clairement attribués au client ayant droit ;

- le client est clairement informé en toute transparence sur l'ensemble des risques (y compris le *slashing*, la période de blocage et les risques en relation avec les incertitudes juridiques actuelles en cas de faillite) ;
- des mesures appropriées sont prises afin de réduire les risques opérationnels résultant de l'exploitation d'un nœud de validation (y compris la gestion de la continuité des affaires), notamment pour éviter le *slashing* et d'autres sanctions ; et
- un *digital assets resolution package* (DARP) est établi aux fins d'une gestion des risques appropriée (voir à ce sujet le chapitre 4.1.1).

En cas de faillite d'un assujetti de la FINMA et lorsque ces exigences sont respectées, la FINMA est actuellement d'avis que les cryptoactifs stakés doivent être systématiquement distraits de la masse au profit des clients déposants conformément à l'art. 37*d* LB en relation avec l'art. 16 ch. 1bis LB.

Cette pratique ne s'applique que temporairement jusqu'à ce que la loi soit clarifiée, qu'une décision judiciaire soit rendue ou que lla situation internationale évolue, ce qui entraînerait une réévaluation de l'interprétation.

4.2 *Direct staking* par des acteurs du marché exerçant sans droit

Concernant les acteurs du marché exerçant sans droit, on considère avec les mêmes réserves d'une clarification législative, d'une décision de justice ou d'une évolution de la situation internationale, que la FINMA supposera en principe qu'il n'y a aucune obligation en matière d'autorisation selon le droit bancaire dans le cas du *custodial direct staking* au nom et pour compte des clients. C'est le cas lorsque les jetons de paiement stakés sont toujours conservés individuellement lors du *direct staking*, c.-à-d. avec une adresse de *blockchain* séparée et attribuable pour chaque client (aux niveaux de l'adresse de conservation initiale, de l'adresse de *staking* et de l'adresse de retrait) et que le prestataire dispose lui-même des clés de retrait. Le dépositaire doit cependant s'affilier à un organisme d'autorégulation pour la surveillance en matière de blanchiment d'argent.

Notons que le *staking* requiert parfois un montant minimal de cryptoactifs (par ex. 32 ETH pour l'Ethereum). Ce montant est souvent élevé afin d'encourager un comportement conforme aux règles de la part des validateurs. C'est la raison pour laquelle les cryptoactifs de différents clients sont souvent collectés sur une adresse de *staking* afin d'atteindre ce montant, notamment lorsque les offres s'adressent à de petits investisseurs. En ce sens, l'offre de services de *staking* implique souvent une conservation collective de jetons de paiements et donc une autorisation selon le droit bancaire.

5 Glossaire

Chaîne de *staking*	L'établissement délègue la responsabilité du *staking* dans le cadre d'une chaîne de *staking* à un prestataire tiers qui assume le pouvoir de disposition sur les clés de retrait (autres banques ou exploitants d'un *pool* de *staking*).
Clés de retrait	Clés cryptographiques permettant de retirer des cryptoactifs stakés, la perte de ces clés entraînant aussi la perte des cryptoactifs stakés.
Conservation collective	Conservation ségréguée de cryptoactifs sur une adresse de *blockchain* collective.
Conservation individuelle	Conservation ségréguée de cryptoactifs sur des adresses de *blockchain* individuelles pour chaque client.
Cryptoactifs	Actifs numériques qui sont répliqués sur une *blockchain* et dont on ne peut disposer qu'au moyen d'une procédure d'accès cryptographique constituée d'une clé publique et d'une clé privée.
***Digital assets resolution package* (DARP)**	Instruction interne visant à informer un liquidateur sur les responsabilités et possibilités d'accès en cas de faillite d'une banque qui conserve des cryptoactifs.
Direct staking	L'établissement pratique lui-même le *staking* et a donc le pouvoir de disposition sur les clés de retrait.
Exploitant d'un (*pool* de) *staking*	Les validations de blocs sont effectuées pour le compte de tiers avec des cryptoactifs de tiers. Si le validateur utilise conjointement des cryptoactifs de différents clients, on parle de *pool* de *staking*.
Exploitant d'un nœud de validation	Exploitant direct d'un nœud de validation de la *blockchain*, soit en tant qu'exploitant d'un (*pool* de) *staking*, soit en tant que prestataire technique.
Jetons de paiement / cryptomonnaies	Cryptoactifs qui servent effectivement ou selon l'intention de l'organisateur ou de l'émetteur de moyens de paiement à l'acquisition de biens ou de services ou au transfert d'argent ou de valeurs (voir aussi à ce sujet l'art. 5*a* al. 1 OB et le guide pratique sur les ICO du 16 février 2018).
Période de blocage/sortie	Durée minimale du *staking* avant que les cryptoactifs ne puissent de nouveau être débloqués ou période entre l'émission de l'ordre d'*unstaking* et le retrait effectif des cryptoactifs stakés.

Prestataire technique	Responsable de la configuration technique (composantes matérielles et logicielles) pour procéder à la production de blocs. Le prestataire n'est en relation qu'avec le validateur et non avec les clients du *staking*.
Slashing	Procédé lors duquel les cryptoactifs stakés sont entièrement ou partiellement détruits en raison d'un comportement problématique du validateur.