Premiers éléments d'analyse de la CNIL

BLOCKCHAIN

Septembre 2018

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Blockchain : quelles solutions pour un usage responsable en présence de données personnelles ?

La Blockchain est une technologie au potentiel de développement fort qui suscite de nombreuses questions, dont parfois celle de sa compatibilité au RGPD. C'est pourquoi la CNIL s'est saisie de ce sujet et propose des solutions concrètes aux acteurs qui souhaitent l'utiliser dans le contexte d'un traitement de données personnelles. La Blockchain est une technologie sur laquelle peut s'appuyer un traitement de données à caractère personnel, et non pas un traitement ayant une finalité à part entière.

1. Qui est responsable de traitement dans la Blockchain ?

Le RGPD, et plus généralement les principes classiques de la protection des données, ont été conçus dans un monde où la gestion des données est centralisée au sein d'entités déterminées. À cet égard le modèle décentralisé de gouvernance des données de la technologie Blockchain et la multiplicité des acteurs intervenant dans le traitement de la donnée complexifient la définition des rôles de chacun.

La CNIL constate toutefois que **les participants**, qui ont un droit d'écriture sur la chaîne et qui décident de soumettre une donnée à la validation des mineurs peuvent être considérés comme **responsables de traitement**.

En effet, les participants à une Blockchain déterminent les finalités (les objectifs poursuivis par le traitement) et les moyens mis en œuvre (format de la donnée, recours à la technologie Blockchain, etc.).

Plus précisément, la CNIL est d'avis que le participant est responsable de traitement :

- lorsqu'il est une personne physique et que le traitement de données personnelles est en lien avec une activité professionnelle ou commerciale (c'est—à-dire lorsque l'activité n'est pas exclusivement personnelle) ;
- lorsqu'il est une personne morale et qu'il inscrit une donnée à caractère personnel sur la Blockchain.

Par exemple si un notaire enregistre le titre de propriété de son client dans une Blockchain, il est responsable de traitement. En outre, si une banque inscrit les données de ses clients dans une Blockchain dans le cadre de ses traitements de gestion des clients, elle est responsable de traitement.

2. Tous les acteurs qui interagissent sur une Blockchain sont-ils responsable de traitement ?

Non. Les mineurs se limitent à la validation des transactions que lui soumettent les participants et n'interviennent pas sur l'objet de ces transactions: ils ne déterminent donc pas les finalités et les moyens à mettre en œuvre.

Par ailleurs, les personnes physiques qui inscrivent des données à caractère personnel dans la Blockchain, en dehors d'une activité professionnelle ou commerciale, ne sont pas responsables de traitement (en application du principe d'exception domestique prévu à l'article 2 du RGPD).

Par exemple, une personne physique qui procède à la vente ou à l'achat de Bitcoin pour son propre compte n'est pas responsable de traitement. Elle peut en revanche être considérée comme responsable de traitement si elle procède à ces transactions dans le cadre d'une activité professionnelle ou commerciale, pour le compte d'autres personnes physiques.

3. Que se passe-t-il si plusieurs participants décident conjointement de mettre en œuvre un traitement sur une Blockchain ?

Lorsqu'un groupe de participants décide de mettre en œuvre un traitement ayant une finalité commune, la CNIL recommande que le responsable de traitement soit identifié en amont. Par exemple, les participants peuvent créer une personne morale sous la forme d'une association ou d'un GIE. Elles peuvent également choisir d'identifier un participant qui prend les décisions pour le groupe et de le désigner comme responsable de traitement.

À défaut, tous les participants pourraient être considérés comme ayant une responsabilité conjointe, conformément à l'article 26 du RGPD et devront donc définir, de manière transparente, les obligations de chacun aux fins d'assurer le respect de la règlementation.

Il est nécessaire que les personnes concernées (i.e. celles dont les données à caractère personnel sont enregistrées sur la Blockchain) sachent vers quelle entité se tourner pour un exercice effectif de leurs droits et que les autorités de protection disposent d'un point de contact qui puisse rendre des comptes sur le traitement mis en œuvre.

S'agissant des *smart contracts*, comme pour tout logiciel, le concepteur de l'algorithme pourra être un simple fournisseur de solution ou, lorsqu'il participe au traitement, être qualifié de sous-traitant ou de responsable de traitement en fonction de son rôle dans la détermination des finalités.

A retenir

- La CNIL considère que le participant pourra dans un certain nombre de cas être qualifié de responsable de traitement :
    - lorsqu'il est une personne physique et que le traitement est en lien avec une activité professionnelle ou commerciale ;
    - lorsqu'il est une personne morale qui inscrit une donnée à caractère personnel;
- lorsqu'un groupe d'organismes décident de mettre en œuvre un traitement sur une Blockchain pour une finalité commune :
    - la CNIL recommande que les participants prennent une décision commune quant à la responsabilité de traitement :
        - soit en créant une personne morale et en la désignant comme responsable de traitement ;
        - soit en désignant le participant qui prend les décisions pour le groupe comme responsable de traitement.
    - à défaut, tous les participants sont susceptibles d'être regardés comme ayant une responsabilité conjointe.

4. Y-a-t-il des sous-traitants au sens du RGPD dans une Blockchain ?

Oui, comme par exemple les développeurs de « smart contract », qui traitent des données à caractère personnel pour le compte du responsable de traitement.

A titre d'illustration, un développeur de logiciel propose à une compagnie d'assurance une solution sous la forme d'un « smart contract », qui permet d'automatiser l'indemnisation de passagers lorsque leur vol a pris du retard dans le cadre de contrats d'assurance voyage. Ce développeur sera qualifié de sous-traitant pour le compte de la société d'assurance, responsable de traitement.

Il est également possible de considérer dans certains cas les mineurs comme des sous-traitants au sens du RGPD. En effet, ils exécutent les instructions du responsable de traitement lorsqu'ils vérifient que la transaction respecte des critères techniques (par exemple un format et une certaine taille maximale, et que le participant est en capacité, vis-à-vis de la chaîne, d'effectuer sa transaction).

Ils devraient donc établir avec le participant, responsable de traitement, un contrat précisant les obligations de chaque partie et reprenant les dispositions de l'article 28 du RGPD (pour en savoir davantage sur les obligations du sous-traitant, cliquer ici).

Par exemple, si plusieurs compagnies d'assurance décident de créer une Blockchain à permission pour leur traitement ayant pour finalité le respect de leurs obligations légales de connaissance client, elles peuvent décider que l'une d'entre elle est responsable de traitement. Dans ce cas, les autres compagnies d'assurance, qui valident les transactions seront susceptibles d'être considérées comme étant mineurs et donc sous-traitants.

⚠ Consciente de certaines difficultés pratiques que peut engendrer la qualification de mineurs en tant que sous-traitant dans la Blockchain publique (notamment en ce qui concerne l'obligation de contractualiser les relations avec le responsable de traitement), la CNIL mène actuellement une réflexion approfondie sur cette question. Elle encourage les acteurs à avoir recours à des solutions innovantes leur permettant d'assurer une conformité avec les obligations que fait peser le RGPD sur le sous-traitant.

A retenir

Dans une Blockchain, le sous-traitant au sens du RGPD peut être :

- le développeur de « smart contract » qui traite des données à caractère personnel pour le compte du participant, responsable de traitement ;
- les mineurs qui valident l'enregistrement de données à caractère personnel dans une Blockchain.

Dans le cas de la Blockchain publique, la CNIL mène actuellement une réflexion et encourage le développement de solutions permettant un encadrement des relations contractuelles entre participants/responsables de traitement et mineurs.

Comment minimiser les risques pour les personnes lorsque le traitement s'appuie sur une Blockchain ?

1. Mener une réflexion préalable sur la nécessité d'avoir recours à une Blockchain, notamment publique

Les caractéristiques de la Blockchain ne sont pas sans incidences sur le respect des obligations découlant du RGPD. Dans le cadre de ses obligations de *Privacy by Design* (article 25), le responsable de traitement doit réfléchir, en amont, à la pertinence du choix de cette technologie pour la mise en œuvre de son traitement.

En effet, la Blockchain n'est pas forcément la technologie la mieux adaptée pour tout traitement de données ; elle peut être source de difficultés pour le responsable de traitement dans le respect des obligations imposées par le RGPD.

Par exemple, la question des transferts hors de l'Union Européenne (UE) peut s'avérer particulièrement problématique, notamment dans le cadre d'une Blockchain publique.

Pour rappel, toute transaction sur la chaîne de blocs implique :

- un envoi à tous les mineurs de la Blockchain d'une demande de validation d'une transaction (et donc potentiellement de données personnelles) ;
- une mise à jour de la Blockchain par l'ajout du nouveau bloc dans la chaîne de bloc auprès de tous les participants.

Or, les participants, qu'ils soient mineurs ou non, peuvent être situés dans des pays en dehors de l'UE. Se pose donc la question du respect des obligations en matière de transferts hors UE (pour plus d'information voir la page « Transférer des données hors de l'UE »).

S'il apparaît qu'il existe des solutions pour encadrer les transferts dans une Blockchain à permission, telles que les clauses contractuelles types, les règles d'entreprises contraignantes, les codes de conduite ou encore les mécanismes de certification, la CNIL constate qu'elles sont plus difficiles à mettre en œuvre dans le cadre d'une Blockchain publique, dans la mesure où le responsable de traitement peut difficilement exercer un contrôle sur la localisation des mineurs.

A retenir

- Si les propriétés d'une Blockchain ne sont pas nécessaires pour atteindre l'objectif, la CNIL recommande de privilégier d'autres solutions permettant d'assurer une entière conformité avec le RGPD.
- Il convient de privilégier une Blockchain à permission qui permet d'avoir une meilleure maîtrise sur la gouvernance de la donnée personnelle, s'agissant notamment des transferts hors UE.
- Les solutions existantes permettant d'encadrer les transferts hors UE, tels que les règles d'entreprises contraignantes ou les clauses contractuelles types, sont entièrement applicables dans la Blockchain à permission.

2. Bien choisir le format sous laquelle la donnée sera inscrite

Le principe de minimisation des données exige que les données collectées soient pertinentes et qu'elles soient limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Par ailleurs, les données personnelles ne peuvent être conservées de façon indéfinie : une durée de conservation doit donc être déterminée en fonction de l'objectif poursuivi par le traitement de données.

Or, l'une des caractéristiques de la Blockchain réside dans le fait que les données qui y sont inscrites ne peuvent être techniquement modifiées ou supprimées : une fois que le bloc auquel est intégrée une transaction a été accepté par la majorité des participants, une transaction ne peut plus en pratique être modifiée.

Certaines solutions techniques, présentées ci-dessous, méritent d'être évaluées par les acteurs afin de remédier à cette difficulté.

> La CNIL mesure l'intérêt de ces solutions mais s'interroge à ce stade sur leur aptitude à assurer une conformité entière au RGPD. Ce sujet fait partie des questions sur lesquelles une réflexion européenne s'avère indispensable.

Pour rappel, la Blockchain peut contenir deux grandes catégories de données à caractère personnel :

Les identifiants des participants et des mineurs :

Chaque participant a un identifiant composé d'une suite de caractères alphanumériques qui semblent aléatoires et qui constituent la clé publique du compte du participant. Cette clé publique se rapporte à une clé privée que celui-ci est le seul à connaître (pour plus d'informations sur la cryptologie et le chiffrement, cliquez ici).

L'architecture même de la Blockchain fait que les identifiants seront toujours visibles, car ils sont indispensables à son bon fonctionnement.

La CNIL considère donc qu'il n'est pas possible de les minimiser davantage et que leurs durées de conservation sont, par essence, alignées sur celles de la durée de vie de la Blockchain.

Les données complémentaires (ou « la charge utile ») :

Outre l'identifiant des participants, les données complémentaires stockées sur la Blockchain peuvent contenir des données à caractère personnel, d'ailleurs potentiellement relatives à des personnes autres que les participants et mineurs.

Pour rappel, le principe de protection des données dès la conception (article 25 du RGPD) nécessite que le format choisi soit celui ayant le moins d'impact sur les droits et libertés des individus.

La CNIL considère que les données à caractère personnel devraient être enregistrées dans la Blockchain, de préférence sous la forme d'un engagement cryptographique[1]. Si cela n'est pas possible, un enregistrement sous la forme d'une empreinte obtenue avec une fonction de hachage à clé est possible, ou, a minima, d'un chiffré, permettant d'assurer un haut niveau de confidentialité.

Le principe commun à certaines de ces solutions est que la donnée en clair est stockée ailleurs que sur la Blockchain (comme par exemple sur le système d'information du responsable de traitement) et que seule une information prouvant l'existence de la donnée y est stockée (engagement cryptographique, empreinte issue d'une fonction de hachage à clé etc.).

Si la finalité du traitement le justifie et qu'une analyse d'impact a démontré que les risques résiduels sont acceptables, des données peuvent exceptionnellement être enregistrées sur la Blockchain sous la forme d'une empreinte classique (sans clé) voire en clair. En effet, certains responsables de traitement peuvent avoir une obligation légale de rendre publiques et accessibles, sans limitation de durée, certaines informations : dans ce cas particulier, un stockage des données à caractère personnel sur une Blockchain publique peut être envisagé, sous réserve qu'une analyse d'impact permette de conclure que les risques sont minimes pour les personnes.

A retenir

- Dans la mesure où les identifiants des participants, c'est à dire leurs clés publiques, sont essentiels au bon fonctionnement de la Blockchain, la CNIL constate qu'il n'est pas possible de les minimiser davantage; leur durée de conservation est alignée avec celle de la Blockchain;

- En ce qui concerne les données complémentaires, afin d'assurer le respect des obligations de protection des données dès la conception et par défaut, et de minimisation des données, la CNIL recommande de privilégier les solutions dans lesquelles la donnée est traitée en dehors de la Blockchain ou, par ordre de préférence, que soit stocké sur la Blockchain :
  - un engagement cryptographique ;
  - une empreinte de la donnée obtenue par une fonction de hachage à clé ;
  - un chiffré de la donnée.

- Si aucune de ces solutions ne peut être mise en œuvre, et lorsque cela est justifié par la finalité du traitement et qu'une étude d'impact a démontré que les risques résiduels sont acceptables, les données peuvent être stockées soit avec une fonction de hachage sans clé soit, en l'absence d'autres possibilités, en clair.

[1] Un « engagement cryptographique » est un mécanisme qui permet de figer une donnée de telle sorte qu'il soit possible, avec des éléments supplémentaires, de prouver ce qui a été figé, et à la fois impossible de la retrouver ou de la reconnaître à partir de cette seule version « engagée »

Comment assurer un exercice effectif des droits ?

Le RGPD a été pensé pour redonner aux individus le contrôle sur leurs informations personnelles. Il renforce donc considérablement les droits des individus par rapport à ceux qui exploitent leurs données et créé, par ailleurs, de nouveaux droits (pour une explication sur les droits des personnes à l'ère du RGPD, cliquer ici)

Outre la minimisation des risques pour la personne, vue précédemment, le format choisi pour inscrire la donnée sur une Blockchain peut permettre de faciliter l'exercice des droits des personnes.

Si l'exercice effectif de certains droits ne semble pas poser de difficultés, l'application du droit à l'effacement, du droit de rectification et du droit d'opposition à la Blockchain méritent une analyse plus détaillée.

1. Les droits entièrement compatibles avec la Blockchain

Le droit à l'information des personnes ne pose pas de difficultés particulières : le responsable de traitement participant devra ainsi fournir une information concise, aisément accessible et formulée en des termes clairs à la personne concernée avant de soumettre à validation des mineurs une donnée à caractère personnel.

Il en va de même en ce qui concerne le droit d'accès et le droit à la portabilité : la CNIL considère que l'exercice de ces droits est compatible avec les propriétés techniques de la Blockchain.

2. Des solutions techniques pour l'exercice des droits permettant de se rapprocher d'une conformité au RGPD

La CNIL constate qu'il est techniquement impossible de faire droit à la demande d'effacement de la personne concernée lorsque des données sont inscrites dans la Blockchain. Toutefois, lorsque la donnée inscrite sur la Blockchain est un engagement, une empreinte issue d'une fonction de hachage à clé ou un chiffré utilisant un algorithme et des clés conformes à l'état de l'art, le responsable de traitement peut rendre la donnée quasi inaccessible, et se rapprocher ainsi des effets d'un effacement de la donnée.

Par exemple, les propriétés mathématiques de certains engagements cryptographiques2 peuvent garantir qu'à la suppression des éléments permettant sa vérification, il ne sera plus possible de prouver ou de vérifier quelle information avait été engagée. L'engagement en lui-même ne présente plus alors aucun risque en termes de confidentialité. L'information devra aussi être supprimée des autres systèmes où elle aura été stockée pour le traitement;

[2] Lorsqu'un engagement cryptogaphique est parfaitement indistinguable (« perfectly hiding »), la suppression du témoin et de la valeur engagée est suffisante pour anonymiser l'engagement de telle façon à ce qu'il perde sa qualification de donné à caractère personnel.

Un autre exemple est celui de la suppression de la clé secrète de la fonction de hachage qui aura un effet similaire. Il ne sera plus possible de prouver ou de vérifier quelle information avait été hachée. L'empreinte ne présentera plus, en pratique, de risque sur la confidentialité. L'information devra, ici aussi, être supprimée des autres systèmes où elle aura été stockée pour le traitement.

En dehors du cas spécifique de certains engagements cryptographiques, ces solutions ne constituent pas un effacement de la donnée au sens strict dans la mesure où les données existeraient toujours sur la Blockchain. Néanmoins, la CNIL constate qu'elle permet de se rapprocher de l'exercice effectif de son droit à l'effacement pour la personne concernée. Leur équivalence avec les exigences du RGPD doit être évaluée.

Il est techniquement impossible de faire droit à la demande de rectification ou d'effacement de la personne concernée lorsque des données en clair ou hachées sont inscrites dans une Blockchain. Il est donc fortement recommandé de ne pas inscrire une donnée à caractère personnel en clair sur la Blockchain, et de privilégier le recours à un des procédés cryptographiques mentionnés.

Concernant le droit à la rectification, l'absence de possibilité de modification des données inscrites dans un bloc doit conduire le responsable de traitement à inscrire la donnée mise à jour dans un nouveau bloc. En effet, une transaction ultérieure peut toujours annuler la première transaction, même si la première transaction apparaîtra toujours dans la chaîne. Les mêmes solutions qu'en cas de demande de suppression de la donnée à caractère personnel pourraient être appliquées à la donnée erronée si elle doit être supprimée.

L'approche est quelque peu différente, bien qu'elle nécessite, comme pour les autres droits, une réflexion en amont, en ce qui concerne le droit à la limitation (instaurée par l'article 18 du RGPD) et à une intervention humaine dans le cadre de la prise d'une décision entièrement automatisée (article 22 alinéa 3).

Par exemple il serait possible d'arriver à une limitation de l'utilisation des données dans les smart contracts, simplement en le prévoyant en amont dans le programme.

Il apparait que la décision entièrement automatisée provenant d'un smart contract est nécessaire à son exécution, dans la mesure où elle permet de réaliser l'essence même du contrat (ce pourquoi les parties se sont engagées). En ce qui concerne les mesures appropriées, la personne concernée devrait pouvoir obtenir une intervention humaine, d'exprimer son point de vue et de contester la décision après que le smart contract ait été exécuté. Il convient donc que le responsable de traitement prévoie la possibilité d'une intervention humaine qui permette de remettre en cause la décision en permettant à la personne concernée de contester la décision, même si le contrat a déjà été exécuté, et ceci indépendamment de ce qui est inscrit dans la Blockchain.

A retenir

- Le droit à l'information, le droit d'accès et le droit à la portabilité ne posent a priori pas de difficultés particulières liées à la technologie Blockchain.
- Comme pour la minimisation des risques, le choix du format de stockage de la donnée via un procédé cryptographique permet de se rapprocher d'un exercice des droits effectif pour la personne concernée : la suppression des données stockées en dehors de la Blockchain et des éléments permettant la vérification permet de couper l'accessibilité à la preuve enregistrée sur la Blockchain, en la rendant difficile voire impossible à recouvrer ;
- Une prise en considération des droits au programme en amont de la mise en œuvre d'un *smart contract* permet d faire droit à une demande de limitation du traitement ou d'intervention humaine.
- L'équivalence de ces solutions avec les exigences résultant du RGPD, notamment en ce qui concerne la limitation de durée de conservation et le droit à l'effacement, suppose une évaluation approfondie.

Quelles sont les exigences en matière de sécurité ?

Les différentes propriétés de la Blockchain (transparence, décentralisation, infalsifiabilité, désintermédiation) reposent en grande partie sur deux facteurs : le nombre de participants et de mineurs, et un ensemble de fonctions cryptographiques d'autre part.

Dans le cas des Blockchain à permission, la CNIL recommande d'évaluer, en fonction de l'éventuelle divergence ou convergence des intérêts des acteurs participants, un minimum de mineurs permettant d'assurer l'absence de coalition permettant de contrôler plus de 50% des pouvoirs sur la chaîne.

La CNIL recommande également de mettre en place des procédures techniques et organisationnelles pour limiter l'impact sur la sécurité des transactions de l'éventuelle défaillance d'un algorithme (notamment cryptographique), y compris un plan d'urgence à mettre en œuvre permettant de modifier les algorithmes lorsqu'une vulnérabilité est identifiée.

Par ailleurs, il convient de documenter la gouvernance des évolutions du ou des logiciels utilisés pour créer des transactions et miner, et de prévoir des procédures techniques et organisationnelles pour assurer l'adéquation entre les permissions prévues et la mise en pratique.

Une vigilance particulière devrait être portée sur les mesures mises en œuvre pour assurer la confidentialité de la Blockchain si celle-ci n'est pas publique.

Tout responsable de traitement mettant en œuvre son traitement via des transactions sur une Blockchain, doit assurer la sécurité des clés secrètes mise en œuvre, en assurant par exemple leur stockage sur un support sécurisé.