ICANN81 | Réunion générale annuelle – Comment ça marche : technologies de noms de blockchain
Dimanche 10 novembre 2024 – 13h15 à 14h30 TRT

YAZID AKANHO : Bien s'il vous plaît, veuillez prendre place. Nous allons commencer dans une minute. Merci.

Bonjour à tous. Je vois qu'il y a encore des gens qui entrent dans la salle. Nous sommes sur le point de commencer, donc veuillez vous asseoir.

Donc au cours de cette séance qui va commencer, nous allons d'ailleurs lancer l'enregistrement.

Bonjour à tous et bienvenue à cette séance « Comment ça marche : technologie de noms de chaînes de blocs ». Donc je suis Yazid Akanho, et je serais le gestionnaire de cette séance.

Cette séance dépend des normes de comportement de l'ICANN et nous appliquons la politique antiharcèlement.

Pendant cette séance, les questions et commentaires ne seront lus à haute voix que s'ils sont soumis dans la partie des questions et des réponses sur Zoom. Et le service d'interprétation pour cette séance va inclure l'anglais, le français, l'espagnol, l'arabe et le turc, et le russe.

Si vous souhaitez prendre la parole pendant cette séance, levez la main sur Zoom. Et lorsqu'on vous donnera la parole, allumez votre micro et prenez la parole. Les participants sur place pourront utiliser un micro

qui est ici dans la salle. N'oubliez pas de donner votre nom, de dire dans quelle langue vous allez parler si vous n'allez pas prendre la parole en anglais, et parlez à une vitesse raisonnable.

Je donne maintenant la parole à Paul. Paul Hoffmann, vous avez la parole.

PAUL HOFFMAN : Bien. J'espère que vous êtes tous ici pour entendre parler de la technologie des noms de domaine de blockchain. Bienvenue à tous, et je vais commencer par exprimer ma satisfaction de voir qu'il y a beaucoup de gens dans la salle. Je pense que vous allez commencer à avoir un petit peu un avant-goût de ce qu'est le système de blockchain. Notre séance va durer une heure, assez courte. Notre présentation ne sera pas trop longue, comme ça, nous aurons le temps de prendre des questions à la fin. Nous allons couvrir le thème de blockchain et des systèmes de nom de blockchain. L'objectif ici est que la communauté de l'ICANN qui est intéressée par les systèmes de blockchain comprenne aussi ce qu'ils sont. Par conséquent, nous allons couvrir d'abord le thème des blockchains, et ensuite nous parlerons de la façon dont le système de noms de domaine de blockchain fonctionne. Nous allons nous centrer sur cela. Mais je serai bref de façon à ce qu'on ait le temps ensuite de prendre des questions.

Alors, je vais commencer par les publications faites récemment par l'ICANN. Vous le connaissez peut-être. Mais comme les gens sont très intéressés par ce système de noms de domaine de blockchain et comme on entend vraiment des opinions très différentes et que l'on

promeut ces différents systèmes de nom de domaine de blockchain, la communauté a posé des questions sur ces thèmes.

Et donc, les questions sont de deux types. Qu'est-ce que c'est ces systèmes de noms de domaine. On a l'habitude du DNS, c'est pour ça c'est ce qu'on fait ici normalement. Alors pourquoi et dans quelle mesure ces noms de domaine sont différents. Et pourquoi ils s'appellent blockchain ? Pourquoi ils s'appellent système de noms de domaine de blockchain. Donc qu'est-ce que c'est qu'une blockchain ?

Alors il y a quelques semaines, nous avons publié deux documents. Et je suis l'auteur de ces deux documents. Et ces documents se trouvent dans la série des documents OCTO. Vous les voyez ici sur l'écran. Et si vous regardez dans la série des documents OCTO, vous allez les trouver. Vous aurez le lien sur le site Internet de l'ICANN. Et vous avez donc ces deux publications qui sont les plus récentes.

OCTO039 va porter sur les technologies de système de noms de blockchain, et OCTO40 sur la blockchain.

Donc vous pouvez les lire tous les deux. Il y a peut-être ici beaucoup de gens ici qui ne sont pas intéressés par le système de noms de domaine de blockchain, mais qui sont intéressés par la blockchain en elle-même. Ces documents sont techniques et neutres, de façon à ce qu'il n'y ait pas de promotion. Et beaucoup de gens n'aiment pas les blockchains. Donc je pense que c'est important. Ces documents sont techniques et sont neutres. Et la raison de cela, c'est que les blockchains et le système de noms de domaine de blockchain évoluent en permanence. Donc si vous aimez quelque chose aujourd'hui, peut-être que demain, vous ne

l'aimerez pas lorsque ça sera transformé en autre chose, ou le contraire aussi. Le contraire peut être vrai. Vous pouvez dire donc cela n'est pas pris encore à être utilisé et puis ce sera le contraire dans le futur. Donc voilà. Si vous les avez lus, c'est bien ; sinon vous pouvez les lire pendant la semaine prochaine.

Une chose que je n'ai pas mise ici sur la diapo, c'est que je suis l'auteur de ces deux documents. Les sources que j'avais pour ces deux matériels, ces deux documents, sont la documentation que j'avais et qui provenait de la communauté de la blockchain et de la communauté du système de noms de domaine de blockchains.

Alors cette documentation est assez mauvaise, incohérente, etc. Donc j'ai mis certaines excuses dans ces deux documents en disant que je me trompe peut-être, il y a peut-être certains faits qui ne sont pas corrects. Donc nous allons refaire une version de chacun de ces documents dans six mois. Donc, si vous trouvez des erreurs, dites-le-moi. Jusqu'à maintenant, c'est sorti il y a deux semaines et personne ne m'a dit qu'il y avait des grosses absurdités. Mais bon. Ici, je vous demande de reprendre peut-être ces documents dans six mois. Il y aura peut-être des modifications. Donc il y a peut-être aussi des choses que les gens ont du mal à comprendre. J'ai aussi trouvé des différences de terminologie.

Bien. Nous allons maintenant parler de la technologie de la blockchain et ensuite nous parlerons du système de noms de domaine de blockchain.

Une des choses intéressantes que j'ai découvertes lorsque j'ai fait cette

recherche sur les blockchains est le fait que les gens me disent oui, je sais ce que c'est que la blockchain. C'est un registre. C'est une base de données. C'est comme la cryptographie.

Et je dirais que c'est faux. Les raisons pour lesquelles cela est faux, c'est que ce système, cet écosystème de blockchain essaie de confondre, de créer le plus de confusion possible. Ils ne font pas ça pour vous embêter. Ils font ça pour faire davantage de sous, d'argent. Alors, on le comprend. C'est quelque chose qui a lieu dans beaucoup de parties de l'écosystème Internet. Pour ceux d'entre vous qui ont mon âge, vous vous souvenez peut-être dans les années 90, on avait la même chose avec les technologies du Web. En 1995, par exemple, un exemple typique c'est que beaucoup de gens disent que les blockchains sont juste une base de données ; mais non. Les blockchains, c'est beaucoup plus qu'une base de données et beaucoup moins qu'une base de données en même temps.

Donc l'objectif de cette séance – il y a une autre séance qui va avoir lieu mercredi – l'objectif ici, et l'objectif de ces documents aussi, est d'essayer de réduire les doutes. Et dans ce sens, nous allons utiliser des terminologies différentes, peut-être, que celles qui sont utilisées par les communautés de la blockchain. Alors, pour deux raisons. D'abord, la terminologie, en général, qui est utilisée par la communauté de blockchain est principalement une terminologie autopromotionnelle, d'autopromotion, de promotion. Un petit peu ce qu'on disait tout à l'heure quand on parlait d'Internet dans les années 90 ; on utilisait des termes. Eh bien, c'est la même chose aujourd'hui. En plus, comme ce n'est pas une communauté très bien coordonnée, ils utilisent les

mêmes termes avec différents sens.

Donc des fois, j'en prends un et je dis voilà ce que ça veut dire pour moi. Et puis, pour être très clair, la plupart des intérêts qui existent concernant la blockchain concernent les finances, les monnaies, etc., le bitcoin, etc. Donc je ne vais pas parler de ça parce que ce n'est pas ce qui intéresse la communauté de l'ICANN. Donc on parle ici de la partie des noms de domaine.

C'est un thème très intéressant. Plus on rentre dans ce thème, plus on s'intéresse à ce thème. Et nous allons ici parler de blockchain et des parties les plus importantes, les parties techniques qui sont les plus importantes de la blockchain.

Alors, d'abord, le registre. On sait tous ce qu'est un registre, même si on n'a pas utilisé un registre. On sait que les banques ont des registres, des journaux dans lesquels ils notent certaines choses. On ne peut pas les couper. On ne peut pas les réécrire. Eh bien, les blockchains sont faites justement selon cette idée d'un registre. Si vous pensez à un registre bancaire, en général, on dit, ce compte a fait passer 50 USD vers cet autre compte, etc.

Alors cela fonctionne comme ça pour la blockchain, pour les transactions de la blockchain. Mais certaines blockchains, comme ethereum , vont permettre que les transactions soient des programmes, des programmes informatiques qui comprennent des choses telles que, par exemple, si cette personne transfère cela, si elle a trop d'argent ou pas assez d'argent, elle va vers ceci ou cela. Donc ce sont des informations qui sont écrites ici. Et c'est beaucoup plus

compliqué qu'un registre bancaire. Mais si vous pensez au terme de registre, à cette idée de registre, même dans le cas de la banque, vous ne pouvez pas regarder au milieu du registre et voir combien de personnes [a]. Vous devez regarder l'ensemble des mouvements pour comprendre ce qui s'est passé. Dans le cas de la banque, une entrée n'est pas Paul a envoyé 50 USD à Yazid, et ensuite Paul à 50 USD en moins dans son compte. C'est juste Paul a envoyé 50 USD à Yazid. Il faut lire la totalité du registre pour suivre vraiment les transactions que Paul a réalisées.

Donc on a un registre. Et donc on a aussi une base de données qui contient toutes ces données.

Là ici, cela est très important dans le domaine -- dans le monde des blockchains, parce que toutes ces transactions peuvent être compliquées. Par exemple, une des transactions typiques auxquelles on ne pense pas dans les banques, c'est quelqu'un a ouvert un compte sans argent. Et c'est quelque chose qui arrive tout le temps dans le monde de la blockchain. Ce compte est arrivé dans l'air, et c'est une transaction déjà. Et ce qui est intéressant dans ce monde des blockchains, par rapport au registre papier, c'est que les règles sont très spécifiques. Si vous prenez une copie du registre et vous voulez comparer, si vous avez deux registres et vous les comparez, vous aurez exactement les mêmes résultats. Et vous pouvez dire exactement ce qui est le bilan de Paul. Et pour les deux. Si vous faites cela sur des ordinateurs différents, vous aurez la même réponse.

Donc cela dit, certaines de ces blockchains représentent des centaines de millions de transactions. Donc obtenir ces registres demande

beaucoup de temps sur Internet. Et faire fonctionner ce registre aussi, le mettre à jour. Ce n'est pas seulement passer un chiffre d'un endroit à l'autre, c'est qu'on a un programme ici. Donc les programmes sont déterminants. Ils n'ont pas de chiffres ici au hasard. C'est-à-dire que si on a 52 personnes ou 50 personnes qui regardent les mêmes blockchains, qui utilisent les mêmes transactions avec les mêmes machines, les machines configurées de la même façon, obtiendront toujours la même réponse. Leurs bases de données auront exactement le même aspect. On ne veut pas qu'on donne tant d'argent à une personne – c'est comme à la banque si on n'a pas assez d'argent. Mais les personnes qui utilisent les blockchains. Quand on a invité ce registre 200 ans après l'invention du registre des banques, on a pu mettre en place ce type de système.

Alors, prochaine diapositive.

La prochaine chose qui est importante dans la technologie des blockchains, c'est une chose qu'on a du mal à admettre. Je dirais que personne ne veut l'admettre. C'est la question qui est basée sur la confiance ; la confiance entre différentes blockchains est totalement différente.

Dans une banque, quand vous regardez le registre, vous pensez que la banque a écrit tout cela de manière peut-être incorrecte et que vous pouvez ne pas leur faire confiance. Mais dans le cas des blockchains, vous devez faire confiance. Une fois que ça a été écrit dans le registre, c'est comme cela. Vous pouvez proposer une transaction en disant je transfère ces monnaies à Yazid, mais si vous avez passé une monnaie, vous allez avoir confiance et vous allez savoir que si tout le monde qui

traite ce registre dit, en même temps, je n'ai pas assez de monnaie pour donner cela à Yazid, à ce moment-là, je vais rejeter cette transaction.

Il y a certaines blockchains dans lesquelles on a une autorité centralisée. Mais on dit aussi que les blockchains sont décentralisées. Il y a beaucoup d'acronymes. Et on parle beaucoup d'acronyme qui commence par un D qui veut dire décentralisé. Vous allez voir que je n'ai pas défini le mot décentralisé ici, parce qu'il y a énormément de définitions de décentralisé.

Différentes blockchains ont des systèmes de modèle de confiance pour leur système de décentralisation. Certaines dépendent d'une base de données ; d'autres dépendent de transactions, de qui fait la transaction. Par conséquent, on peut être un peu moins restrictif en ce qui concerne la base de données, la façon dont on transforme cela en une base de données.

Et les blockchains peuvent être mises à jour, ce qui va demander beaucoup d'énergie, d'électricité ici. Et les exemples les plus communs, les plus courants de cela, c'est le bitcoin. C'est comme ça que ça a commencé, par le bitcoin.

Et cela a un coût électrique très élevé de rentrer toutes ces transactions. C'est un processus très très lent également. L'ethereum a un coût bien moindre, parce que les transactions peuvent aller beaucoup plus vite. Cela ne veut pas forcément dire que l'ethereum est meilleur que les bitcoins. Certaines personnes parmi nous pourront dire qu'ils sont intéressés par les générations futures et le changement climatique, mais c'est plus une question du modèle de confiance avec lequel ces

devises fonctionnent.

Chaque devise au départ de la blockchain ont déterminé qui doit être – à qui on fait confiance, combien de temps on met pour faire confiance.

Donc dans ces exemples que je vous ai donnés, par exemple, un bloc de transactions arrive dans le monde du bitcoin. Les personnes ne font pas confiance à cela tant que neuf autres personnes ont dit – ont vérifié ce bloc pour s'assurer que c'était une réalité. L'ethereum ne prend que cinq ou six personnes pour vérifier cela. Encore une fois, les personnes qui comparent l'ethereum et le bitcoin se basent là-dessus. Mais ce sont deux systèmes complètement différents.

Si on prend les systèmes de nommage basés sur la blockchain. Ce sont des systèmes différents également. Nous ne voulons pas attendre une heure pour voir notre nom apparaître. Et alors, je ne peux pas vous dire quels types de système de nommage basé sur la blockchain sont les meilleurs ou pas. Tout dépend de vos priorités.

Donc voilà une description assez brève du fait que les blockchains sont vraiment différentes. Même les modèles de confiance sont différents entre différents types de blockchains.

Donc encore une fois, il y a également différents types de couches, de blockchain de couche. ethereum et bitcoin sont des blockchains de couche 1. Les blockchains de couche 2 sont beaucoup plus flexibles. Et vous vous rendrez compte que les propositions de système de nommage basé sur la blockchain sont des systèmes de couche 2. Cela permet d'augmenter la confiance dans ces informations, puisque nous prenons des informations de la couche 1 et nous nous assurons

d'arriver vers une couche 2 pour s'aligner entre les deux couches.

Il peut y avoir également des dates inscrites dans ces informations. Cela devient complètement fou très rapidement avec ces différentes couches.

Et nous avons également des chaînes de blocs qui sont autonomes, qui peuvent être utilisées à part. Et certains systèmes de nommage utilisent ces blocs autonomes qu'on appelle des chaînes latérales, des *side chains*. Et si vous gérez une *side chain*, vous n'avez que vous-même à convaincre. Cependant, il faut que les autres utilisateurs aient confiance en vous également.

Par exemple pour les banques, si je suis une banque qui est basée seulement à un endroit très spécifique, personne ne me connaît et personne ne peut me faire confiance. Mais je pourrais ouvrir une banque, ouvrir un compte dans des banques qui sont connues de tous.

Donc encore une fois, ce sont des modèles de confiance bien différents. Si je vous dis envoyez-moi de l'argent sur ce compte dont vous n'avez jamais entendu parler, ou veuillez m'envoyer de l'argent sur ce compte dont vous avez peut-être déjà entendu parler que vous pouvez trouver ailleurs, ou si je vous dis envoyez-moi de l'argent sur ce compte dont vous avez déjà entendu parler, encore une fois, c'est une question de confiance. Et la blockchain est basée sur cette idée où nous avons différents modèles de confiance qui veulent dire différentes choses.

Et la vraie question c'est est-ce que vous pensez que cela existera à l'avenir. Ces questions de blockchains sont basées sur des registres ouverts à tous, qui sont disponibles dans le domaine public. La question

de la confiance, c'est est-ce qu'on fait confiance à ces modèles, à ces transactions qui sont gérées avec succès, pour s'assurer que personne n'utilise cela à mauvais escient.

Alors dernière diapositive.

Certaines personnes entendent la blockchain et pensent immédiatement à la cryptographie. Alors, mettez cela de côté. Pardon, je vais être très direct, mais j'ai de l'expérience de la cryptographie. La cryptographie qu'on utilise est bonne, mais elle n'est pas très intéressante. Ça ne change pas grand-chose par rapport à la cryptographie qu'on utilise depuis 25 ans déjà.

Encore une fois, beaucoup de promotion sur la blockchain est adressée à des personnes qui ne savent pas ce que c'est. Et si on utilise ce type de cryptographie, je vous dirai seulement ça, mais ils utilisent de la cryptographie très bonne, mais elle n'est pas intéressante.

Ceci étant dit, il y a tellement d'argent qui est injecté dans l'écosystème de la blockchain que parfois certains cryptographes essaient de travailler sur des nouvelles choses qui peuvent être utilisées dans les blockchains. Ce n'est pas encore complet. Ce n'est pas encore finalisé. Certaines idées sont très bonnes, mais cela prend beaucoup de temps. Et cela s'améliorera peut-être à l'avenir. Mais pour le moment, pour les blockchains, et d'ailleurs c'est une très bonne chose si vous ne comprenez pas la cryptographie. Moi je comprends très bien que ce ne soit pas à la portée de tout le monde.

Si vous êtes intéressé par la cryptographie, venez me voir. J'ai des références à vous donner, de très bons livres. Mais si quelqu'un vous dit

que la blockchain est meilleure que certaines autres manières de fonctionner parce qu'elles utilisent une bonne cryptographie, c'est faux.

Alors, désormais passons donc à la blockchain maintenant que vous avez compris ce qu'était la blockchain. Parlons désormais de la technologie en elle-même.

Parce que chaque système de nommage des blockchains décide de ses propres règles, il est impossible de dire que ce type de blockchain peut être comparé avec ce type de blockchain et a tels avantages, tels inconvénients. Les règles changent constamment. C'est comme si vous ouvrez un restaurant qui dit cuisine chinoise. Vous pouvez transformer cela en cuisine chinoise et thaïe si c'est ce qui intéresse vos clients. Vous n'avez pas besoin de changer votre nom. Ou vous pouvez changer votre nom et toujours servir de la cuisine chinoise. C'est toujours acceptable.

Les systèmes de nommage blockchain s'appellent toujours des systèmes blockchain en fonction de ce dont ils ont besoin. Et c'est même bien plus simple pour eux de s'appeler le DNS mondial, et de dire également que le DNS mondial change les règles de manière très lente. Mais la blockchain est autonome. Et donc il est difficile de déterminer quelles sont les règles sur ce système de blockchain en particulier ou tel autre système.

La technologie blockchain qui est utilisée ne fait pas l'objet de beaucoup de documentation. Elle n'est pas très recherchée. Certains systèmes de blockchain utilisent un type de blockchain qui peut vous être inconnu. C'est comme si je vous disais, encore une fois, envoyez-

moi de l'argent sur ce compte d'une banque dont vous n'avez jamais entendu parler. Encore une fois, ça peut être très bien pour vous. Mais si vous ne savez même pas de quelle banque je vous parle, en particulier parce que ma banque a le même nom qu'une autre banque dans un autre État des États-Unis, par exemple, parce que, par exemple, il y a des banques aux États-Unis qui sont des banques différentes, mais qui ont le même nom – qui s'appellent Bay Area ; il y en a cinq différentes qui ont le même nom. Mais encore une fois, vous ne savez toujours pas quel est le modèle de confiance de cette chaîne de bloc. Vous ne savez pas si vous pouvez lui faire confiance. Et c'est un peu pareil si on se concentre sur la technologie qui nous intéresse.

Maintenant qu'on a parlé de cette question de la confiance, on va parler de la manière dont les systèmes de blockchain de nommage fonctionnent. C'est pour cela que vous êtes là d'ailleurs à cette réunion de l'ICANN.

La première chose à laquelle on pense dans le DNS mondial, c'est qu'est-ce qui est résolu lorsque je cherche un nom sur Internet. Vous avez tous suivi les cours disponibles sur le DNS. Donc, lorsque l'on cherche ICANN.org, vous cherchez une adresse IPv – IPv4 ou IPv6. Ce que vous trouvez lorsque vous résolvez le nom d'une adresse, ce n'est pas en réalité une adresse – alors ce qu'ils appellent dans le système de blockchain, c'est une adresse de portefeuille, mais ce n'est pas une adresse et ce n'est pas un portefeuille. Cela vous amène sur la blockchain qui a créé le nom. Ça a du sens, et c'est ce qui est le plus utile dans le monde de la blockchain. Si vous dîtes à quelqu'un, je veux que vous m'envoyiez de l'argent, plutôt que de retenir une chaîne de

caractères ou une chaîne de chiffres qui est mon adresse personnelle et ma clé personnelle, vous pouvez juste envoyer une adresse. C'est assez similaire au DNS mondial où vous cherchez un nom et vous arrivez sur une adresse IP.

C'est assez similaire, mais en réalité la différence c'est l'utilisation primaire des systèmes de nommage sur les blockchains. Alors, je vous ai dit plusieurs fois qu'il y a différents types de blockchain, il y en a des milliers en réalité. Donc votre adresse sur une chaîne de bloc, sur une blockchain, sera différente de votre adresse sur une autre chaîne blockchain. Lorsque vous cherchez à résoudre un nom, il faut trouver vos différentes adresses. Par exemple, si j'ai un portefeuille ethereum , un portefeuille bitcoin et un portefeuille d'une autre blockchain, il faut chercher tout ce qui va s'adresser – tout ce qui vous correspond.

Un autre aspect qui est mis en avant par les systèmes de chaîne de bloc par rapport au système du DNS, c'est que toutes les transactions qui rentrent dans ces blockchains sont publiques et elles sont stockées de manière permanente sur la blockchain. Vous pouvez trouver qui a créé cette blockchain, quand est-ce qu'elle expire, est-ce qu'elle expire – parce que certains systèmes de nommage expirent, certains n'expirent pas, qu'est-ce qui a été changé. Toutes ces informations sont publiques et sont faciles à trouver. Elles sont difficiles à digérer, mais elles sont faciles à trouver. Et ça, c'est quelque chose que nous n'avons pas à offrir dans le DNS mondial.

Nous avons l'opportunité de le faire. Tous les bureaux d'enregistrement, les opérateurs de registre peuvent créer des registres et les rendre publics. Mais il n'y a pas beaucoup de demandes pour cela.

Dans le monde de la blockchain, vu que les registres sont à la base de ce système de décentralisation, il y a une demande d'accès à toutes ces informations. C'est donc un aspect absolument fondamental.

Et ce n'est pas tout. L'un des autres aspects qui est considéré comme un avantage du système de nommage basé sur la blockchain, c'est-ce que vous pouvez acheter votre nom de domaine sur la blockchain avec la devise de la blockchain. Donc vous pouvez directement acheter avec du bitcoin.

Encore une fois, votre adresse de portefeuille est ce qui vous permet de payer. Certains disent par exemple que si vous achetez un nom de domaine de deuxième niveau sur un gTLD avec une carte de crédit, votre carte de crédit, le nombre de votre carte de crédit n'est pas public, mais il est associé de manière permanente avec votre nom. Dans cette salle, vous n'allez peut-être pas forcément comprendre ce que je veux dire. La communauté blockchain recherche cela ; ils veulent savoir qu'une personne a acheté ce nom de domaine avec tel compte pour pouvoir le garder. Encore une fois, certains systèmes de blockchain sont sur la base d'un achat unique et la propriété est indéfinie. Si vous achetez par exemple avec des bitcoins, vous créer un compte bitcoin et vous utilisez de l'argent normal et vous en tirez des bitcoins. Ce compte, encore une fois, a une clé publique, et vous avez une clé privée. Et si vous perdez votre clé privée, c'est dur pour vous, mais c'est votre problème. Non seulement vous n'avez plus accès à ce compte, mais c'est que ce compte est indéfini.

Et il est difficile de mesurer exactement ce qu'il y a sur ce compte. Mais les recherches montrent que 70 % des comptes sur les bitcoins sont

morts. Donc certains d'entre eux ont plus d'argent que moi, mais même s'ils ont un petit montant, ils pensent que ça n'a plus d'importance. Donc il y a un compte qui est associé avec un nom de blockchain. Et ça va rester dans certains systèmes de noms de domaine. Dans d'autres systèmes de noms de domaine, comme le DNS mondial, vous devez renouveler cela tous les ans.

Et le dernier point ici sur la diapositive, qui va peut-être donner lieu à beaucoup de questions, est si on a un système de noms de domaine de blockchain, il doit avoir un nom. Donc, certains utilisent un TLD, qui [son]t des chaînes qui ne sont pas actuellement déléguées. Donc on a [ET] et [TH]. Il y en a d'autres, beaucoup de cryptoportefeuilles. Et ils ne sont pas actuellement dans le DNS global. Ils ne figurent pas dedans.

Donc si vous avez un nom comme par exemple .ETH ou dans mon cas P.Hoffmann.ETH, pour pouvoir trouver les données qui sont associées avec cela, vous devez demander au résolveur qui possède – qui connaît cet ETH. Et dans le cas du portefeuille, le *wallet*, il y a deux systèmes de noms différents. Donc je peux ici avoir un P.Hoffmann.wallet ici et un autre nom ici.

Donc beaucoup de systèmes de noms de domaine blockchain utilisent ces alt TLD, ce TLD alternatif. Ce qui donne lieu à beaucoup de questions. Est-ce qu'ils sont alloués ; est-ce qu'ils ne sont pas alloués ? Est-ce qu'il y a deux ou quatre ou sept systèmes de noms de domaine de blockchain avec le même nom ? Comment est-ce qu'on fait pour les résoudre ?

Donc, c'est un petit peu chaotique. Et c'est justement l'intérêt qu'il y a

ici, parce que le DNS mondial a été tellement bien organisé, puisqu'on parle ici du fait qu'il n'y ait pas de problème, qu'il n'y ait pas eu de problèmes pendant plus de 35 ans. Donc, comme on a l'habitude de cette stabilité du système du DNS, le système de noms de domaine de blockchain est différent. Nous n'avons pas besoin de cela. Nous voulons une décentralisation qui peut être liée à beaucoup de chaos. Mais peu importe.

Et le dernier point ici aborde la question des systèmes de noms de domaines qui peuvent coordonner avec le DNS mondial en utilisant des noms qui sont en réalité déjà dans le DNS mondial. Ils peuvent faire cela en étant liés ou en reliant les noms de DNS dans la blockchain – premièrement ici, deuxièmement, là-bas, ou vice versa.

Donc c'est un marché qui est plus petit, mais qui est très intéressant, parce que maintenant on prend des noms que l'on connaît. Et on a aussi une résolution alternative quelque part ailleurs. Actuellement, on a l'habitude d'utiliser le nom de domaine mondial, le système de DNS mondial. Mais on peut avoir différents résolveurs avec différentes capacités. Certains vont avoir DNSSEC, d'autres non. Il y a beaucoup de résolveurs donc qui font que si on leur donne un nom, si on donne un nom à un site ou à une adresse dont on ne veut pas entendre parler pour différentes raisons, ils vont arriver quand même à mentir, à biaiser et à exister. Donc c'est ce type de choses qui existent dans le nom de blockchain.

Les noms sont les noms. Vous pouvez enregistrer quelque chose ici et ailleurs. Ils vont autoriser des noms qui ne sont pas dans le DNS mondial.

Et comment ça fonctionne ? Voilà, c'est la question ; c'est la grande question. Je crois que c'est l'heure. Donc je vous propose de passer aux questions. Nous avons le temps. Yazid va organiser cela. Vous avez un micro dans la salle. Mais je veux vous dire une chose. Si vous me dîtes comment le système de noms de domaine blockchain fonctionne avec ceci ou cela, je dois vous le dire ; je ne vais pas vous expliquer cela. Et même si je pouvais le faire, ça demanderait beaucoup de temps. Donc on ne va pas faire ça. Rappelez-vous aussi que les chaînes de bloc ou les blockchains en eux-mêmes sont très différentes. Et les modèles de confiance aussi sont très différents. Donc il y a des questions auxquelles je ne vais pas pouvoir répondre, parce que ces communautés changent en permanence ce qui a lieu actuellement. On a l'habitude du système de DNS mondial stable, qui fonctionne normalement avec des changements lents, et ce n'est pas la même chose. Mais si vous demandez comment est le système de DNS mondial aujourd'hui, si on le compare avec ce qu'il était il y a 10 ans, on va constater une évolution. Dans le cas de la blockchain, et dans le cas du monde de la blockchain, les choses dans 10 ans seront totalement différentes pour différentes raisons. C'est important de le dire.

YAZID AKANHO : Merci, Paul, pour cette excellente présentation. Je pense que nous avons le temps pour les questions. Nous avons une quarantaine de minutes.

Donc je vous rappelle si vous êtes dans la salle, vous avez le micro qui est dans le couloir central de la salle. Si vous ne parlez pas en anglais, s'il vous plaît, dites-nous dans quelle langue vous allez parler, donnez

votre nom et dites la langue dans laquelle vous allez parler. Pour ceux qui nous suivent à distance, nous vous demandons d'utiliser la partie des questions et des réponses sur Zoom.

Bien, alors on va regarder s'il y a des questions dans la salle. Bien s'il vous plaît, allez-y. Vous êtes à côté du micro. Vous pouvez y aller. Vous êtes le premier.

SAM YILMAZ : Merci. Merci Paul. Très intéressante votre présentation. Je suis Sam Yilmaz, et j'appartiens à l'espace blockchain de [inaudible].

Donc OCTO39 et OCTO40 essaient d'être neutres et de nous informer. Mais si vous dîtes, voilà les normes qui sont proposées par et soutenues par ICANN, est-ce que cela est soutenu par la blockchain, alors, qu'est-ce que vous en pensez ? Est-ce que vous pensez qu'on peut soutenir cette nouvelle technologie ? Est-ce qu'on peut demander davantage de transparence ? Est-ce qu'on peut demander des transactions avec des intermédiaires ? J'aimerais entendre votre réponse.

PAUL HOFFMAN : Je suis navré. Je vous remercie pour cette question, mais je suis navré ; je vais vous décevoir. Je fais partie du personnel de l'ICANN. Donc mon opinion ne compte pas. C'est l'opinion de la communauté qui compte. Il y a certaines choses que la communauté va peut-être dire qui vont me paraître catastrophiques. Mais peu importe. Ce sont des questions de la communauté. C'est pour cela que j'ai dit, c'est moi qui ai écrit OCTO39 et OCTO40. Je fais partie du personnel de l'ICANN et le personnel de

l'ICANN doit comprendre aussi ce type de choses. Mais l'objectif ici c'était que la communauté le lise et puisse prendre certaines décisions à propos des blockchains.

Donc pour répondre spécifiquement à votre question, comment est-ce que les blockchains peuvent être intégrées en tant que telles, nous avons 1300 gTLD qui sont actuellement sous contrat. C'est quelque chose – environ 1300. Donc certains peuvent choisir aussi d'avoir des interactions avec la blockchain. Certains peuvent passer directement à la blockchain. Certains veulent effleurer la blockchain. Certains ne veulent pas en entendre parler.

Et ensuite, on a la prochaine série de nouveaux gTLD, dont on parle beaucoup actuellement. Et comment est-ce que cela va affecter la prochaine série ? Que veut la communauté pour la prochaine série ? Et peut-être que la prochaine série arrive trop vite pour pouvoir prendre ce type de décision politique que vous souhaitez. Et à ce moment-là, les personnes qui vont participer à la prochaine série vont être affectées par ce que ces gTLD peuvent donner – transformer, si on passe à une autre technologie.

Alors, je serai honnête ici. Et c'est mon opinion. C'est une prédiction, mais ce n'est pas ma spécialité. Ce n'est pas quelque chose que je sais faire normalement. Mais en tout cas ce que je prédis, c'est qu'on va bientôt voir des ccTLD qui ne seront pas sous contrat de l'ICANN, qui vont faire certaines choses et qui vont faire des recherches qui vont découler des ccTLD. Donc la moitié peut montrer la moitié de ses recherches afin de nous montrer les bonnes choses ; et l'autre moitié, les mauvaises choses.

Donc ce n'est pas quelque chose en ligne droite. Moi, ce que j'essaie, c'est de vous montrer un petit peu les deux côtés de la question. Je pense qu'on va voir cela au niveau de la communauté des ccTLD justement, ces deux aspects. Ne demandez pas au personnel de l'ICANN de donner son opinion sur ce type de choses. J'ai bien sûr ma propre opinion. Mais ça ne compte pas. Ce qui compte, c'est l'opinion de la communauté. Et c'est l'opinion de la communauté qui va nous montrer le chemin pour l'ICANN.

YAZID AKANHO : Merci Paul. Nous avons une autre question. Allez-y.

OSCAR GIUDICE : Bonjour. Je suis Oscar Giudice, de l'Uruguay. Je vais parler en espagnol.

Donc un système – donc on va parler en espagnol. Vous devriez mettre vos casques. Voilà, le monsieur a mis son casque. OK, bien. Vous êtes prêts ? Alors on y va.

Merci. Merci pour cette présentation, Paul. C'était très intéressant. Si j'ai un système de DNS qui fonctionne avec un système de chiffrage de cryptologie A et un système qui fonctionne avec un système de cryptologie B, et j'ai deux noms, ces deux noms sont enregistrés dans les deux systèmes. Est-ce que je vais devoir modifier le résolveur dans ce DNS mondial ? Est-ce que je dois tout recommencer ? Parce que ça veut dire qu'il faut tout jeter à la poubelle et tout refaire.

PAUL HOFFMAN : C'est compliqué. Je m'excuse. Je ne parle pas votre langue. Je suis un de ces Américains qui ne parlent pas l'espagnol. C'est une bonne question.

Nous ne devons pas faire quelque chose. Nous sommes encouragés à être le plus larges possible. Mais on ne doit pas faire quelque chose. Si quelqu'un a un système de noms alternatifs qu'il nous propose, cette personne doit nous montrer comment cela va améliorer le DNS mondial. C'est eux qui doivent nous expliquer comment cela doit être séparé ou intégré dans le DNS mondial. C'est à eux de le faire donc.

On sait déjà ce qui se passe. Il y a des nouvelles idées. Il y a des résolveurs ; résolveur A, résolveur B. Tout cela, ça dépend de votre propre choix. Et on va peut-être trouver un moyen de faire marcher tout cela et de faire fonctionner tout cela ensemble. Et peut-être pas.

Vous avez donné un bon exemple. Vous avez un nom sur un résolveur A et un nom sur un résolveur B ; on ne sait pas si A et B fonctionnent ensemble et correctement. Encore moins s'ils fonctionnent avec le DNS mondial correctement. Donc je pense que la réponse à votre question serait est-ce qu'il faut mettre tout à jour, tous les systèmes à jour ? Et ma réponse serait que non.

Mais on peut peut-être vouloir le faire. Il y a peut-être des choses qui vont surgir dans ce système de noms de domaine blockchain, qui sont intéressantes. Donc je l'ai déjà dit. Il y a de nombreux systèmes de noms de domaine blockchain qui existent. Vous avez parlé d'un système qui peut être sur A, un autre qui peut être sur B. Certains peuvent être meilleurs – meilleurs pour la communauté de l'ICANN et meilleurs pour

le DNS mondial comme nous le connaissons ; meilleurs ou moins bon.

Donc nous allons, je l'espère, faire des changements avec ceux qui sont les meilleurs. Mais il faut d'abord comprendre lequel est le meilleur. Et peut-être, A et B sont bons tous les deux. Et C et D et E ne sont pas bons. Donc c'est le système de noms de domaine blockchain qui doit venir nous voir et nous dire, voilà comment on aimerait faire les choses ; voilà comment nous, on fait les choses. Est-ce que la communauté de l'ICANN veut participer ou pas ?

Donc c'est encore un peu tôt peut-être. C'est un peu précoce. Je vous remercie.

YAZID AKANHO : Merci beaucoup. Dernière question dans la salle, puis nous répondrons aux questions des participants en ligne.

INTERVENANT NON IDENTIFIÉ : Merci beaucoup. Merci pour votre présentation. Je suis désolé. Je n'ai pas lu OCTO039 et OCTO040, donc peut-être que vous y avez déjà répondu. Je m'appelle [inaudible]. Je représente la communauté et le droit. Je vais parler en anglais.

Une partie de mon travail est d'évaluer les risques, surtout sur les technologies très complexes, telles que celles-ci. Nous avons beaucoup de questions.

Le système actuel présente des enjeux, des problèmes, surtout lorsqu'il s'agit d'enregistrements. Et donc je serais très curieux de savoir si, de

votre point de vue très objectif, cette technologie présente des risques vis-à-vis de cela ou est-ce qu'il est trop tôt pour le dire.

PAUL HOFFMAN : Oui. Prochaine question ? Non, pardon. Merci pour votre question, mais je vais changer votre question un petit peu.

Est-ce que je pense que les technologies de nommage sur la blockchain présentent des risques différents par rapport à ceux auxquels nous faisons face pour le moment ? La réponse est oui, absolument, en particulier due à cette nature décentralisée, puisque, dans ce cas-ci, la décentralisation veut dire que personne ne prend la responsabilité.

Vous pouvez créer un nom de domaine sur le système blockchain, vous pouvez demander à trois personnes de s'enregistrer, puis, en tout cas pour ethereum par exemple, vous pouvez créer un contrat qui dit je suis un nom de domaine. Et pour enregistrer votre nom de domaine, vous pouvez payer des frais pour faire cela. Je vais mettre en œuvre un résolveur là-dessus, et tout le monde peut l'utiliser. Et ensuite, vous pouvez vous en aller. Un contrat sur une blockchain ne requiert pas de travail d'aucune partie.

Donc si le système est légitime et utilisé, et que le créateur l'abandonne, ou s'il échoue, par exemple, ce contrat est toujours en œuvre. Il est toujours vivant.

Il y a donc des plus grands risques sur les systèmes de nommage, même si l'objectif était de créer de bonnes choses, d'empêcher l'utilisation malveillante, d'empêcher des falsifications, etc. Mais si les personnes

abandonnent leur contrat, leur contrat reste valide et reste applicable à l'avenir. Et cela pose donc énormément de risque. Et, à chaque fois que vous essayez d'intégrer deux systèmes différents, des systèmes de nommage différents, il y a des différences. On ne peut pas avoir deux choses complètement identiques ; on peut faire le maximum pour qu'elles se ressemblent, mais on ne peut pas avoir une ressemblance exacte.

Donc, de mon point de vue, ces types de risque sont énormes, puisque le DNS mondial a déjà 30 ans de règles derrière lui. Les systèmes de nommage de blockchain n'ont que trois ans d'existence. Et pour des raisons de profit sur le DNS mondial, en particulier pour les gTLD, par exemple, il y a un équilibre avec les ccTLD. Et parce que nous avons ces opérateurs de registre et ces bureaux d'enregistrement. Et ça, c'est quelque chose qui n'existe pas dans ce système de blockchain.

Donc nous avons l'habitude de certains risques. Peut-être que pour vous c'est encore trop de risque, mais nous les comprenons. Mais si nous ne comprenons pas les risques présents dans ce nouveau système, c'est un risque en soi. Donc bien sûr que nous avons des risques. Cela ne veut pas dire que cela sera une catastrophe si nous utilisons ce type de technologie, mais ce sont des risques à prendre en compte.

Et encore une fois, si on revient à la première question quelles sont mes opinions là-dessus, je suis une personne. Mon opinion serait de le faire le plus simple possible. Vous êtes une grande communauté. Vous avez réfléchi à ces questions depuis plus longtemps. Donc vous avez la capacité de faire cette analyse des risques, et de manière bien plus

exacte qu'un seul individu.

YAZID AKANO : Merci Paul. Nous allons passer maintenant aux questions en ligne. Nous avons quelques questions de la part de Fouad Bajwa. Donc nous allons poser la première question.

Tout d'abord, merci beaucoup à Paul d'avoir créé ces documents. Nous n'avons pas beaucoup de documentation là-dessus. C'est très utile. Est-ce que Paul a pensé à créer un groupe de travail sur la technologie des systèmes de nommage sur la blockchain.

PAUL HOFFMAN : Merci beaucoup. La réponse est non. Encore une fois, ce n'est pas au personnel d'organiser notre travail, c'est à la communauté. Je suis persuadé que certains membres de la communauté voudront créer un groupe de travail tel. Et je suis persuadé que trois quarts des personnes dans cette salle voudraient courir en hurlant face à ce type de groupe de travail, parce que le sujet est très fluide et très changeant. Et il serait très difficile de créer un groupe de travail qui pourrait fixer quelque chose dans le temps. Si c'est le souhait de la communauté, c'est parfait. N'hésitez pas à parler aux membres du Conseil, aux membres du personnel, mais nous, en tant que membres du personnel, nous n'avons pas prévu de créer cela.

YAZID AKANHO : Merci beaucoup Paul. Question de Fouad.

Comment est-ce que vous gérez les noms de TLD actuels ? Comment est-ce qu'ils sont gérés ? Comment est-ce qu'ils sont reconnus dans le DNS mondial s'ils ne sont pas reconnus par l'IANA ?

PAUL HOFFMAN : C'est une très bonne question. Ils ne le sont pas. Ils ne sont pas reconnus par IANA. Donc, nous ne les voyons pas. Cela veut dire que nous n'utilisons pas les résolveurs – qu'ils n'utilisent pas nos résolveurs. Donc nous ne les voyons pas. Il y a des possibilités d'utiliser différents types de résolveur, soit avec des alternatives différentes. Certaines requêtes peuvent être demandées à différentes de résolveur, et les solutions sont disponibles, sont accessibles, mais encore une fois, nous avons l'habitude du DNS mondial. Nous savons comment il fonctionne. Nous savons comment gérer ces résolutions. Nous savons comment réguler les systèmes de nommage, ces serveurs de nommage. Mais pour tous les autres serveurs, ils n'apparaissent pas dans le DNS.

Donc si vous demandez à un résolveur du DNS mondial une requête sur ce type de TLD, vous n'aurez pas de réponse. Encore une fois, certains résolveurs commencent à mettre en œuvre des réponses là-dessus. Parfois, vous pouvez avoir des noms de domaines alternatifs qui ont des réponses puisque certains résolveurs essaient de les intégrer. Mais quel type de réponse vous recevez ? Si vous lancez une requête au DNS mondial, vous cherchez probablement une adresse IP version 4. Une adresse IP version 6. Mais ce que vous pouvez recevoir, ce que vous pouvez recevoir de ces noms de domaine alternatifs pourrait être un nom de compte, par exemple. Donc ce sont des choses complètement différentes,

Encore une fois, si nous avions des accords avec la communauté ICANN et le DNS mondial sur ces systèmes alternatifs, la résolution de ces requêtes sera très difficile. Nous savons résoudre des requêtes dans le DNS mondial. Toutes les normes sont respectées dans le DNS mondial, mais ces normes n'existent pas encore dans ces nouveaux systèmes.

YAZID AKANHO : Merci Paul. Nous avons une ligne sur place. Mais nous allons prendre une question supplémentaire en ligne, puis revenir à la salle.

La prochaine question est de savoir quelle est la position sur les domaines basés sur la blockchain et l'intégration de ces domaines dans le DNS. Est-ce qu'il y a des discussions là-dessus au sein de l'organisation de l'ICANN et de la communauté pour faire face à la compatibilité et la résolution de ces noms de blockchain. Donc en réalité, c'est la question précédente. C'est la même question que la question précédente.

PAUL HOFFMAN : Alors, c'est une bonne question de demander au personnel de l'ICANN des questions de politiques, mais ne demandez pas à quelqu'un comme moi qui est spécialiste de la technologie. Je suis assez convaincu que l'ICANN pour le moment n'a pas de politique. Alors, personne de l'équipe juridique ne s'est levé de sa chaise. Donc je pense que c'est vrai. Nous n'avons pas de politique pour le moment.

Je ne sais pas si nous allons développer une ou pas. Mais la première réponse serait de dire oui, bien sûr, la communauté va travailler sur ces

questions. L'autre réponse pourrait être de dire oh, mon dieu, non, c'est beaucoup trop difficile pour nous, et nous avons beaucoup trop de choses à faire déjà. Une autre réponse pourrait être à quoi bon, puisque les systèmes des blockchains, du nommage de blockchain, ont déjà leur propre écosystème qui fonctionne pour leur propre monde. Le DNS mondial fonctionne pour notre mandat nous, qui est bien plus large et bien plus stable. Mais peut-être que notre réponse serait de dire que nous n'avons pas besoin de nous préoccuper à faire cela puisque c'est bien trop large.

Encore une fois, l'ICANN ne veut pas critiquer l'existence de chaque nom de domaine, que ce soit un nom de domaine basé sur la blockchain ou autre. Nous avons un document qui s'appelle l'ICP3. Est-ce que – oui ICP3. Il est encore bien tôt dans la semaine pour moi. Qui a été développé dans les années 2000, je crois que c'était en 2002, qui disait que nous n'avons pas de politique sur les autres noms de domaine. Et cela a beaucoup de sens en réalité, puisqu'il y a un millier de noms de domaine, de systèmes de noms de domaine. Nous avons un système hiérarchique avec des noms humains, mais les codes postaux par exemple sont un système de nommage. Tout dépend d'où vous êtes, de ce que vous faites et si c'est plus facile à lire ou pas. Mais l'ICANN n'a pas de politique sur les codes postaux. L'ICANN n'a pas de politique sur comment vous appelez vos enfants. Certains pays ont des règles sur la manière dont on peut appeler nos enfants. Ces systèmes de blockchain rentrent dans ces catégories sur lesquelles nous n'avons pas de position ; nous n'avons pas de positionnement politique.

Cela peut changer. La communauté peut décider de changer cela. Vous

pouvez, vous, en tant que communauté, décider de rendre le travail plus simple ou plus difficile. Je ne souhaite pas vous influencer ici, mais il faut le dire. Mais pour le moment, non, nous n'en avons pas. Je pense que si la communauté voudra prendre cela en compte, cela prendra du temps, puisque comme nous l'avons vu, il nous faudra apprendre encore beaucoup de choses avant de pouvoir prendre une position.

Certaines personnes seront peut-être trop fatiguées après avoir appris trop cela. Certaines personnes encore pourraient dire que le DNS va trop lentement, le système blockchain avance beaucoup plus vite, et il faut qu'on commence à y travailler.

YAZID HOFFMAN : Merci Paul. Nous allons passer aux questions dans la salle, mais juste un rappel pour celles et ceux qui sont en ligne. Les questions posées dans le chat ne seront pas considérées comme des questions. Donc utilisez la boîte des questions et réponses s'il vous plaît.

BERTRAND DE LA CHAPPELLE : Bertrand de la chapelle au micro. Bonjour. Je travaille sur le système juridique des réseaux.

Alors deux choses. Déjà, merci beaucoup d'avoir produit ces documents et d'avoir mené cette séance, puisque je pense que cela s'applique à beaucoup de personnes dans la communauté et dans l'At-Large.

La compatibilité et l'articulation entre les systèmes de nommage, c'est un vrai enjeu. C'est quelque chose qui revient très souvent. Vous avez tout à fait raison de dire qu'il faut faire un contraste, une comparaison

entre le système que nous connaissons, qui a 30 ans d'existence, qui est très hiérarchisé, avec ce système–

PAUL HOFFMAN : Alors, permettez-moi de vous arrêter. On peut dire que c'est organisé, mais, en réalité, personne dans le monde du DNS ne dirait que ce que nous avons est organisé. Alors c'est relatif.

BERTRAND DE LA CHAPPELLE : Oui, c'est vrai. Mais ce sont des espaces très différents. Les environnements sont très différents. Et pourtant, après vous avoir félicité sur ces discussions, j'espère que ces discussions continueront lors des réunions.

Cependant, je ne suis pas tout à fait à l'aise avec cette position de recul extrême que vous avez exprimé, parce que cela me pose question sur le rôle de l'ICANN. L'alternative n'est pas entre nous avons une politique, et nous n'avons pas de politique.

Le rôle du personnel – et le rôle très utile du personnel, c'est de pouvoir encadrer ces questions et ces problèmes. Et si nous avons des personnes en dehors de la communauté, comment est-ce qu'on va expliquer de manière très simple qu'un .XYZ est sur le DNS, mais que le point ATH est complètement différent. Je suis désolé si cela se ressemble et nous devons être très clairs.

Donc il y a deux points ici. La première question, c'est ce que l'ICANN peut fournir à la communauté de manière externe. Est-ce que nous avons des leçons à partager avec la communauté ? Est-ce que nous

avons des apprentissages à partager avec la communauté externe qui peuvent les aider à décider de comment ils veulent s'organiser ? Peut-être que certains systèmes de blockchain ne veulent pas faire les choses de la manière dont nous l'avons fait. Mais peut-être que certaines leçons et certains dangers auxquels nous avons fait face peuvent être utiles pour eux.

Et enfin, je pense qu'il est nécessaire d'avoir une discussion très sérieuse sur l'impact potentiel de ces blockchains, en particulier sur la confusion des utilisateurs. Nous parlons beaucoup de la confusion des noms, du risque de créer de la confusion pour les utilisateurs finaux. Donc c'est un sujet très important pour nous. Donc ne voyons pas les choses en noir et blanc. Ce n'est pas une question de la communauté ou du personnel, ou ce n'est pas une question de politique ou pas de politique. Mais nous devons travailler ensemble. Nous devons organiser cette discussion pour savoir comment organiser nos points.

Et je pense que le personnel a beaucoup à apporter, que ce soit du point de vue technologique ou du point de vue politique. Vous pouvez nous aider à organiser notre pensée, et donc savoir comment est-ce que nous pouvons vous aider et comment est-ce qu'on va être impacté.

Donc encore une fois, je ne vous encourage pas à créer un groupe de travail, mais de lancer un processus très clair, pour que chaque réunion de l'ICANN ait une structure dédiée, basée sur les blockchains. Donc continuons cette discussion, c'est très important.

PAUL HOFFMAN : Bien. Vous avez raison. C'est raisonnable en tout cas, et je vous

remercie. Je travaille pour le bureau du CTO. Et dans le CTO, il y a [inaudible] qui dit technique. Mais bon. Le personnel devrait être guidé par la communauté, même pour commencer ce que vous avez dit. Nous n'avons pas besoin d'être vraiment très fortement encouragés. J'ai fait ces deux documents parce que j'ai constaté qu'il y avait là une certaine confusion. Ce n'est pas que le Conseil m'a dit vous devez le faire. Je pense qu'il y a des personnes du côté politique qui pensent la même chose que moi, mais donc qui pourraient parler, eux, de la partie politique.

En tout cas, le cadrage est très important. Mais ici, ce cadrage est très difficile, vu cette grande quantité de systèmes de noms de domaine blockchain. Donc, j'espère que l'OCTO39 va vous aider à mieux comprendre. Peut-être que vous allez avoir certaines fonctionnalités, certaines caractéristiques. Est-ce qu'il y a des choses qui vont être modifiées dans le futur, il y a des choses qui vous préoccupent peut-être ?

Bien. En tout cas, maintenant je vais vous donner mon opinion. Je ne pense pas que le système blockchain donne beaucoup d'importance à tout cela. Ils veulent voir ce qu'ils peuvent faire et si ce n'est pas trop de travail pour eux. Donc j'espère que j'ai tort, mais je pense qu'une des différences que nous allons voir dans la communauté des blockchains, c'est que certains d'entre eux vont interagir davantage de manière plus cohérente avec la communauté de l'ICANN et d'autres vont rester à distance, vont dire OK ça ne marche pas ; bon, c'est bon. C'est comme ça que ça va être fait, je pense. Mais c'est correct. Donc si vous voulez un cadrage du côté de la politique, ne demandez pas cela au technicien.

Mais vous savez qu'il y a du personnel qui s'occupe de la politique ici qui peut le faire.

Je ne sais pas à quelle communauté vous devez demander cela. En tout cas, je pense que ça pourrait être utile que cette discussion ait lieu, et que l'on commence à se pencher sur cette question.

YAZID AKANHO : Eh bien, je dois dire que certaines questions sont difficiles ici. Bien. Allez. On donne la parole à Peter. Allez-y, Peter.

PETER : Merci. Merci beaucoup. Je suis Peter. Donc je voudrais ici parler de l'aspect politique à nouveau. Vous avez dit que l'on ne peut pas imposer certaines choses à la communauté. Mais vous dîtes quand même qu'il y a une conversation concernant la politique qui doive avoir lieu. Alors, est-ce que vous pensez qu'on doit la cadrer cette conversation ? Comment est-ce que cela va affecter la communauté de l'ICANN et tout ce qui concerne la confiance, cet environnement de confiance des [multiparties].

Ensuite, quand vous parlez de la confiance et des modèles de confiance des différents systèmes de blockchain, à mon avis -- ou à votre avis, pardon, quels sont ces modèles de confiance qui sont les modèles qui ne fonctionnent pas bien, qui n'ont pas les droits nécessaires au niveau cryptographique ? Alors qu'en pensez-vous ? Par où commencer ?

PAUL HOFFMAN : Bien. Merci beaucoup. C'est une question difficile. Je vais commencer par la deuxième partie, quels sont mes modèles de confiance préférés.

Bien. J'ai fait cela. Je travaille dans ce domaine depuis 30 ans. Donc moi j'aime bien quand on a un système centralisé, contrôlé, avec un système IANA au milieu ; et ça fonctionne. Mais maintenant, je dois dire que j'ai commencé à travailler dans ce domaine avant IANA, avant ICANN.

Donc il y a eu une ICANN. Il y a une communauté à un moment donné qui a commencé à organiser tout cela.

Ma première réaction au début des années 2000, c'était oh ça va se compliquer -- les choses vont se compliquer. Et maintenant – ensuite, je me suis dit, bon, ça va être peut-être un peu plus compliqué, mais ça veut dire aussi qu'il y a beaucoup de gens qui vont commencer à participer à ce modèle de confiance. Et ce modèle de confiance, au début, c'était celui de Jon Postel. Le modèle de confiance qui a évolué après la mort de Jon et qui a donné lieu à l'ICANN. Au début, j'étais très préoccupé par l'apparition d'ICANN. C'était très chaotique. Mais la communauté l'ICANN nous a montré que l'on pouvait ordonner ce chaos à travers des politiques et des procédures qui, on va tous être un peu d'accord pour dire que chaque politique a été un peu longue à élaborer, mais on a quand même des politiques et une communauté.

Donc je pense que c'est peut-être ce qu'on aimerait voir au niveau des blockchains. Alors il y a quelques tendances qui apparaissent dans le système de noms de blockchain qui voudraient donc choisir leur propre blockchain et établir leurs propres règles. Donc moi personnellement,

je ferai confiance dans certaines règles que j'aime bien, et moins confiance dans d'autres règles.

En tout cas, il faut reconnaître, il y a beaucoup de gens qui aiment bien aller, on laisse le chaos s'installer et on va voir ce qui se passe. Bon. Mais de nouveau, pour revenir à ce que vous avez dit, quand est-ce qu'on commence à ordonner les choses ?

Je ne suis pas vraiment la personne qui va pouvoir vous dire comment vous devez vous en occuper ou si vous devez vous en occuper. N'oubliez pas que plus tard dans la semaine, nous allons faire – mercredi matin, nous allons faire une autre présentation. Comme tous les ans, OCTO va faire une séance qui va s'appeler « Technologies des identificateurs émergents ». Donc on va parler des noms de blockchain et compagnie. Et vous aurez le temps pour poser des questions. Donc venez. Venez mercredi non pas pour m'entendre à nouveau, mais pour entendre les questions qui vont être posées. Je pense que c'est intéressant. En tout cas, les compagnies de nom de blockchain qui sont représentées mercredi ont un modèle qui, si vous ne le connaissez pas, peut vous surprendre et peut vous rassurer aussi. Voilà.

Les politiques évoluent. Elles évoluent mieux ici que dans un grand nombre d'organisations. L'IETF aussi, on pourrait l'inclure ici. En tout cas, on n'a pas à vous dire vous devriez vous consacrer aux blockchains. C'est à vous de choisir. Je sais que beaucoup de gens en ont un petit peu peur, mais c'est toujours pareil pour les décisions politiques. Donc vous devez choisir votre combat, prendre votre temps, et si vous voulez rentrer dans la description des noms de domaine blockchain, je vous soutiendrai au niveau du personnel de l'ICANN.

YAZID AKANHO : Merci Paul. Bradley, est-ce que vous pouvez garder votre question pour la pause-café, s'il vous plaît ? Je vous donnerai la parole. Il nous reste trois minutes. Donc on a des questions en ligne.

« Est-ce qu'il y a des mentions ou des analyses dans ce rapport concernant les temps de requête DNS de blockchain et les temps de réponse ? Si vous n'avez pas cela, est-ce qu'il y a des plans pour le futur ? Je pense que les performances des requêtes DNS sont plus préoccupantes. »

PAUL HOFFMAN : Je vais vous décevoir. Il n'y a pas eu beaucoup de recherche dans ce domaine. Et la raison pour cela, c'est que la résolution a lieu dans ce système de noms de domaine blockchain, de manière décentralisée. [Moralité] ? Pas vraiment, parce que c'est un système. C'est une résolution de nom qui est centralisée. Donc ça va changer, je pense, avec le temps. Ils vont avoir un temps de réponse aux requêtes meilleures dans le temps. Il n'y a pas eu de mesures concernant cela. Je ne fais pas trop confiance dans la capacité d'être mesuré concernant ce temps de réponse.

YAZID AKANHO : Paul, une autre question.

« Est-ce que vous pensez que ce serait une bonne idée de passer du système DNS mondial au système blockchain ? Est-ce que ce serait un – puisque le système mondial demande beaucoup de temps, est-ce que

ce serait une manière d'évoluer ? »

PAUL HOFFMAN : Oui, merci. C'est une question difficile. Mais la réponse est non. Je ne veux pas qu'on passe du système du DNS au système de blockchain. On va commencer par cela. Je pense qu'il y a quelqu'un d'autre qui est d'accord avec moi, d'après ce que j'entends. Mais il va y avoir d'autres changements technologiques sur l'Internet, non pas dans le DNS, quelque chose que je n'ai pas envie de voir non plus, et qui peut être positif. Donc il faut être patient. Donc si ce changement dont vous parlez a lieu, ce n'est peut-être pas quelque chose qui va me plaire, mais je reconnais qu'il faudra être patient et voir. Ça sera peut-être quelque chose de positif.

YAZID AKANHO : Merci Paul. Nous allons – nous avons deux dernières questions. Nous allons demander aux traducteurs de les traduire.

« Même à cette étape précoce, pensez-vous qu'il y a des innovations et des composantes de système de nommage blockchain qui peuvent aider la communauté globale Internet ou améliorer le DNS mondial tel qu'il est considéré par l'ICANN ? Et est-ce qu'il y a une intégration complète qui pourrait être difficile à imaginer à ce stade ? »

Je crois que c'est une question qui vous est posée, Paul.

PAUL HOFFMAN : Merci pour la question, mais je ne suis pas vraiment la bonne personne

ici. C'est de nouveau une question qui doit être posée à la communauté. Je peux trouver le – je peux vous donner la réponse, mais je pense que c'est la communauté qui doit décider ici.

YAZID AKANHO : Et la dernière chose. « Les blockchains, c'est des registres ou le DNS ? »

PAUL HOFFMAN : Bien. Nous n'avons plus le temps. Je dirais merci pour ces questions. Lorsque vous avez un système de nommage qui est différent de ce qu'on a l'habitude d'utiliser dans le DNS mondial, on a des questions de ce type tel que qu'est-ce qu'un registre, qui fait la résolution si ce n'est pas le système de registre, alors ce changement, comment passer d'un système de noms de blockchain à un autre système. Si cette communauté dit à la communauté de blockchain, nous voulons parler avec vous et nous aimerions coopérer avec vous, si ça les intéresse, ils vont coopérer ; ils vont faire des changements techniques et politiques dans ce sens. C'est une conversation avec deux personnes, deux acteurs, deux intervenants.

YAZID AKANHO : Merci Paul. Je vous rappelle, si vous êtes dans cette salle, qu'il va y avoir une autre séance, mercredi matin à 10 heures 30. Vous pouvez regarder dans le programme de l'ICANN. Et donc, n'hésitez pas à venir participer à cette séance mercredi. Les présentations sont aussi à votre disposition sur la page de l'ICANN, là où vous trouvez le programme.

Et je vous remercie et la séance est maintenant levée.

[FIN DE LA TRANSCRIPTION]