ICANN75 | Réunion générale annuelle – Nouvelles technologies d'identificateurs
Mercredi 21 septembre 2022 – 15h00 à 16h00 KUL

ADIEL AKPLOGAN : Notre séance d'aujourd'hui était initialement prévue pour être consacrée aux nouveaux types de systèmes de nommage. Ces nouveaux systèmes de nommage ont déjà été évoqués dans une séance précédente. C'est une séance de suivi actuellement, donc les technologies ont évolué depuis. L'OCTO a aussi produit un document qui examine ces systèmes de nommage alternatifs.

Aujourd'hui, nous allons donner la parole à Alain Durand, qui fait partie de notre équipe de recherche au sein de l'ICANN. Il est l'auteur de l'OCTO-034 qui nous donne un aperçu des défis qui nous concernent et il va nous donner du contexte.

Ensuite, nous allons passer à Luc van Kampen, qui va nous parler du système de noms Ethereum. Et nous aurons une séance de questions réponses avec eux.

La dernière intervention n'est pas directement liée au système de nommage alternatif, mais elle est alignée avec le titre, c'est-à-dire les identificateurs. Cette intervention sera présentée par Jacques Latour de CIRA.

Remarque : Le présent document est le résultat de la transcription d'un fichier audio à un fichier de texte. Dans son ensemble, la transcription est fidèle au fichier audio. Toutefois, dans certains cas il est possible qu'elle soit incomplète ou qu'il y ait des inexactitudes dues à la qualité du fichier audio, parfois inaudible ; il faut noter également que des corrections grammaticales y ont été incorporées pour améliorer la qualité du texte ainsi que pour faciliter sa compréhension. Cette transcription doit être considérée comme un supplément du fichier mais pas comme registre faisant autorité.

Maintenant, nous allons donner la parole à Alain. Alan, vous avez la parole.

ALAIN DURAND : Bonjour ou bonsoir. C'est le matin où je suis et vous êtes en fin d'après-midi à Kuala Lumpur. J'aurais voulu me joindre à vous en présentiel, mais la vie en a voulu autrement. J'espère que vous m'entendez.

ADIEL AKPLOGAN : Oui, nous vous entendons.

ALAIN DURAND : Merci beaucoup.

Aujourd'hui, je vais vous présenter un document que j'ai publié plus tôt dans l'année, l'OCTO-034, sur les défis relatifs aux systèmes de noms alternatifs. Diapositive suivante s'il vous plaît. L'objectif de ce document est d'examiner les systèmes de noms alternatifs et non pas suppléants. Alternatif signifie quelque chose de différent.

Il y a des défis techniques dans le déploiement des systèmes de nommage alternatifs. Notre objectif est l'analyse en profondeur de la façon dont les systèmes de nommage alternatifs fonctionnent. Il ne s'agit pas d'aller dans les processus

d'élaboration de politiques. Nous allons nous consacrer sur l'aspect technique. Il y a un lien qui est à votre disposition et présenté sur la diapositive. Diapositive suivante.

Ces systèmes de nommage alternatifs ne sont pas nouveaux. Certaines racines alternatives ou suppléantes précèdent l'ICANN et la situation n'était pas très claire. Et en 2001, un document a été publié, l'ICP-3, déclarant que ces racines alternatives étaient problématiques. Gardez à l'esprit que ceci n'est pas nouveau. Nous avions déjà ce concept il y a 20 ans. La raison pour laquelle ce concept est remis en lumière, c'est que la popularité des blockchains met en lumière les systèmes de nommage basés sur la blockchain.

Il y a trois systèmes de nommage. Aujourd'hui, il y a le Handshake dérivé des bitcoins. Il y a l'Ethereum et les domaines imparables dérivés de l'Ethereum. Ce qu'il faut savoir, c'est qu'il n'y avait pas d'obligation d'utiliser un système de nommage basé sur la blockchain. On pouvait utiliser le DNS. Les développeurs ont décidé d'aller dans ce sens. C'est la première observation. Diapositive suivante.

Autre chose qui est nouveau, c'est qu'il y a des bureaux d'enregistrement accrédités par l'ICANN qui vendent ces noms basés sur la blockchain. Sachez que les noms de domaine blockchain ne sont pas soumis aux politiques de l'ICANN. Diapositive suivante.

Le déploiement des systèmes de nommage alternatifs. La question qui se pose, c'est comment un utilisateur Internet peut être résolveur de noms à partir d'un système de nommage alternatif ? C'est facile. La véritable question, c'est comment les utilisateurs standards peuvent accéder à ce système de nommage ? Il y a plusieurs façons de procéder. Si vous utilisez une application native, vous pouvez utiliser une bibliothèque dédiée pour arriver à vos fins.

Si vous avez une application héritée, comme un e-mail, un navigateur, il y a des techniques passerelle qui existent. Vous pouvez utiliser un pont URL pour atteindre les domaines qui vous intéressent, vous pouvez utiliser un résolveur local traité par un ISP, vous pouvez utiliser des navigateurs dédiés. Mais toutes ces techniques peuvent être problématiques, surtout si vous dites aux gens d'utiliser un navigateur spécifique ou avec une extension. Ceci peut poser un problème. Cela fonctionnait bien au début, mais les problèmes ont commencé à se poser.

Le défi maintenant, c'est non seulement communiquer à vos clients potentiels un nom, mais il faut aussi leur indiquer ce qu'il faut faire. Vous devez leur dire d'utiliser un navigateur en particulier pour entrer en connexion. Diapositive suivante, s'il vous plaît.

Comme je l'ai dit, cette passerelle peut être réalisée avec des résolveurs récursifs et peut-être que votre IDP peut agir, peut-être

que votre résolveur récursif peut agir, mais il faut faire attention car cela peut conduire à de l'instabilité. Tout dépendra du type de résolveur. Certains sont adaptés pour certaines choses et d'autres, pour d'autres choses. Donc, vous aurez un problème de régularité ou de cohérence.

Par exemple, si vous êtes chez vous, vous avez votre réseau, Wi-Fi, votre réseau cellulaire. En fonction de votre connexion et en fonction de votre résolveur, vous pourrez obtenir des réponses potentiellement différentes. Chez moi, par exemple, j'ai un signal Wi-Fi dans certaines parties de ma maison. Il peut être assez faible et dans une autre partie de ma maison, j'aurais peut-être un réseau cellulaire. Je vais donc choisir en fonction de la force de mon réseau. C'est difficile à expliquer aux utilisateurs lambda. La diapositive suivante, s'il vous plaît.

Ici, il s'agit du déploiement de l'une des alternatives. Qu'en est-il lorsqu'il y en a plusieurs ? Il y en a trois, mais rien ne nous empêche d'en avoir une quatrième ou une cinquième. Le problème, c'est qu'il n'y a pas de coordination axée sur la communauté. Par conséquent, il y a des collisions de noms qui sont inévitables et nous savons que les collisions de noms sont compliquées et elles posent de nombreux problèmes.

L'approche naïve, c'est qu'il faut davantage de systèmes de nommage, car si je ne peux pas obtenir le nom que je souhaite dans un système, alors j'irai dans un autre. C'est très bien, mais

c'est une approche naïve car elle ne répond pas à la question « Comment les gens vont pouvoir vous atteindre ? » Il me suffit d'utiliser une appli, mais l'appli ne peut vous connecter qu'à un système de nommage à la fois. Donc, il faut une appli spécifique pour un espace de noms spécifique. Les choses peuvent devenir assez compliquée. Cela peut conduire à beaucoup d'instabilité. Il y a aussi la question de configuration et ceci peut devenir très difficile. Les utilisateurs finaux qui ne sont pas très compétents en matière technologique auront du mal à naviguer à travers tous ces problèmes. Diapositive suivante.

Il y a un risque et c'est celui de la fragmentation de l'Internet, car il y aurait la création d'écosystèmes séparés, un pour chaque système de nommage. Ci on dit « J'utilise telle famille d'applications, dans une autre situation, j'utilise une autre famille d'applications », elles finiront par ne jamais communiquer l'une avec l'autre et ce n'est pas le résultat que l'on recherche. Diapositive suivante.

Cela nous rappelle le début des années 2000 lorsqu'il y avait cette création dissipée. Vous pourrez lire ce document ICP-3. C'était l'engagement de l'ICANN pour créer un seul DNS racine faisant autorité pour résoudre les problèmes techniques. Le système de nommage alternatif n'est pas forcément basé sur le protocole DNS, mais toutes les thématiques de collision sont les mêmes. Je ne dirais pas que l'ICP-3 doit s'appliquer à ces situations, mais je

dirais qu'il faut être inspiré par cela et il faudrait tirer les enseignements nécessaires. Diapositive suivante, s'il vous plaît.

Les gens parlent de la collision des noms en disant que ce n'est pas très grave. Je vais vous montrer un petit dessin qui va vous permettre de pouvoir observer un scénario afin de voir comment les utilisateurs finaux sont impactés.

Il y a deux personnages dans cette histoire. Il y a John qui est un peu le geek et il y a Sally qui est un peu geek, mais pas autant que John. John dit : « Je veux un nouveau nom de domaine, on peut utiliser un nom de blockchain. Marché, tu peux me vendre un truc cool comme cela ? » Marché : « Je ne peux pas te vendre ce genre de domaine, mais je peux te vendre john.cryptonite. » Et il dit : « Sally, connecte avec moi ici. Voilà, mon nom est john.cryptonite. Et Sally dit : « Bien sûr, il n'y a pas de problème. J'essaie, mais cela ne marche pas. » John répond : « J'ai oublié de vous dire, Sally, que tout d'abord, vous devez installer ce super navigateur Web » et Sally dit : « Je n'en ai jamais entendu parler. Est-ce que ce navigateur est sûr ? »

Un peu plus tard, John le geek dit : « J'ai trouvé cette autre blockchain. Il y a plein de trucs sympas là-bas. Je vais demander à Marché si je peux avoir un nouveau nom de domaine là-bas. » Marché dit : « Je veux bien vous vendre john.superblockchain. » Prochaine diapo.

D'accord. John revient vers Sally et dit : « Hé Sally, j'ai de nouvelles choses à te proposer. Voilà john.superblockchain. » Sally lui répond : « John, j'ai installé ton navigateur spécial comme tu me l'as dit la dernière fois, mais ça ne fonctionne pas avec ton nouveau domaine john.superblockchain. » Alors, John dit : « Sally, j'ai encore oublié. C'est une blockchain différente. Il faut que tu installes cet autre navigateur. Il y a aussi un plugin à télécharger. » Et Sally lui répond : « Mais arrête. »

Un peu plus tard, Sally revient vers John et dit : « John, j'ai finalement suivi toutes les étapes que tu m'avais expliquées et je peux maintenant voir ton adresse john.superblockchain. Mais quand j'essaie john.cryptonite du début, je ne te vois pas. Je vois mon ancien petit ami. » John dit : « Je n'ai rien fait. Regarde, c'est mon profil. »

Comme vous le voyez, les deux voient deux choses bien différentes. John revient vers ce celui qu'il appelle Marché et dit : « Sally n'est pas contente. Comment se fait-il qu'elle et moi voyons des choses différentes quand on tape john.cryptonite ? » Marché dit : « C'est ce qu'on appelle la collision des noms. Cryptonite, c'est un mot populaire. Au moins trois blockchains différentes l'utilisent. Votre ordinateur et le sien ne sont pas configurés de la même façon. Vous regardez dans un espace de noms, elle regarde dans un autre ; pas étonnant que vous voyez des choses différentes. Il n'y a pas de garantie que les noms soient

uniques. Mais john.cryptonite est toujours disponible dans le troisième système de nommage de la blockchain. Voulez-vous l'acheter ou dois-je l'offrir à l'ex-petit ami de Sally ? » John n'est pas content et dit : « C'est stupide, je vais revenir à mon ancien nom de domaine TLD john.icann. Au moins, il était unique. » Marché dit : « Tu ne peux pas échapper à la collision des noms. Le TLD .icann est désormais disponible dans cinq systèmes de nommage alternatifs différents. Peut-être que tu veux créer ton propre système de nommage. » John dit : « Marché, tu es un monstre. L'Internet est maintenant cassé. »

Merci d'avoir écouté ma petite présentation.

ADIEL AKPLOGAN : Merci Alain d'en avoir terminé sur cette note sympathique avec ce petit dessin animé. Dans votre présentation, il avait trois points clés : les défis dus à la résolution, nous avons aussi la confusion de l'utilisateur qui est bien illustrée par votre petit dessin animé. Dans tout cela, il y a un thème sous-jacent, un élément qui peut nous amener vers la fragmentation du DNS en premier et ensuite, la fragmentation de l'Internet au niveau mondial.

Maintenant, nous allons passer à la prochaine présentation. Avant de de passer à la séance de questions et réponses, Luc, je vais vous passer la parole. Vous êtes de l'ENS, un des espaces de

nommage alternatif. Je vais vous donner l'opportunité de partager quelques mots avec nous.

LUC VAN KAMPEN : Est-ce que tout le monde voit mon écran ?

Bienvenue, bonsoir, bon après-midi, que vous soyez ici ou en ligne. C'est bien d'avoir toutes ces personnes autour de la table. Encore une fois, bienvenue à tous ceux qui sont présents, que ce soit sur Zoom ou dans la salle. Je m'appelle Luc van Kampen.

L'Internet évolue tous les jours. En 1989, l'ICANN a été fondée pour clarifier tous les éléments pour l'ordre et la discipline de l'Internet. En 2004, nous avons eu le lancement des réseaux sociaux. Des milliers de sites Web ont été lancés, servant des millions d'utilisateurs. Donc, deux ères bien différentes.

Aujourd'hui, nous avons plus de cinq milliards d'utilisateurs sur l'Internet, 63 % de la population totale. Le monde avance très vite et l'authentification avance aussi vite. On voit qu'il y a un changement super rapide, avec des mots de passe, des clés publiques aussi, qui ne sont pas un mouvement très nouveau. On le voit dans les technologies qu'on utilise tous les jours, HTTPS, SSL, PGP et surtout, DNSSEC. Bien sûr, il y en a d'autres.

Comment cela a un impact sur l'authentification ? Il nous faut résoudre des tas de questions. Il y a des mots de passe qui ne sont

pas sécurisés, des fuites de mots de passe, du piratage des comptes en masse, la disponibilité des noms, etc.

Regardons la dernière diapo de l'autre présentation. Nous avons @icann, @icann.org parce que le Facebook…, il y a aussi le @icann d'Instagram, il y a ICANN photos sur Flickr et ICANN sur SoundCloud. De plus, il y a le site Web de l'ICANN.

Les clés publiques résolvent des tas de questions. Les clés sont utilisées pour identifier les choses sur l'Internet. Regardez, c'est le mien. Les clés privées sont hébergées par un instrument local. Les gens peuvent utiliser ces machines pour signer, pour conformer un message, une transaction bancaire, etc., même pour signer un message. Ils doivent ainsi prouver qu'ils sont qui ils sont en utilisant leur biométrique, que ce soit la confirmation de l'iris, des empreintes, etc.

Le cryptage public, du point de vue de la sécurité, c'est génial parce que cela vous donne une sécurité imparable. Cela prendrait beaucoup de ressources pour pirater un message. Au niveau de de l'élargissement ou de l'extension, c'est fantastique, c'est fait très facilement. Au niveau de la route de l'état de préparation des différentes machines et des dispositifs, c'est très facile parce que tout cela est déjà prédéfini et préinstallé. En dernier, c'est facile à lire pour nous, les êtres humains. Au niveau de la lisibilité, pour les utilisateurs, c'est pratique.

Et voilà où nous rentrons en jeu, l'ENS. Nous voulons intégrer les notifications de clés publiques dans les systèmes de noms de domaine. Cela veut dire que toutes les personnes qui ont un DNS existant peuvent utiliser leur domaine en tant que leur identificateur à travers le Web. Vous avez vu cette diapo avec tous les différents ICANN. On pourrait mettre icann.org partout. Cette petite clé de verrouillage que j'ai mise pourrait aider à signifier que tous les messages seront signés et autorisés. Cela peut se faire par un utilisateur unique, par plusieurs dispositifs ou par plusieurs personnes qui auront à approuver ce qui se fait donc sur les sites Internet.

Ça, c'est moi, luc.computer, un domaine que j'ai enregistré avec un bureau d'enregistrement. C'est mon DNS. Tous les sites Web que je vais aller voir auront cela. Je pourrais toujours voir luc.computer. Et si vous regardez et que vous tapez luc.computer, vous allez me trouver. De quoi est-ce que cela a l'air ? Voilà, ce serait comme cela. Ce sera en haut de la page, dans le coin gauche ou dans le coin droit sur le site Web de l'ENS, comme cela, et bien sûr, sur plusieurs différents serveurs et sur beaucoup d'autres aspects.

En ce moment, 2,4 millions de noms ont été connectés à travers l'ENS, cela fait plus de 600 000 utilisateurs qui sont disponibles sur des milliers de sites Web. Comment cela fonctionne-t-il ?

Comme je n'ai que 10 minutes et que mon temps est limité, je vais essayer d'être bref.

Le service de nommage Ethereum est construit sur une base de données publique qui héberge des informations pour décentraliser. Ethereum utilise des contrats intelligents qui sont essentiellement des codes qui sont logiques, qui sont hébergés dans les blockchains et c'est un ensemble de données qui vous disent comment les données seront partagées, tous les services qui seront appliqués et cela nous permet d'avoir toutes les informations sur les blockchains.

Comment est-ce que ceci se produit ? Les contrats intelligents, mon nom, mon nom de domaine, mon adresse publique, c'est ce que j'utilise à travers le monde, et bien sûr beaucoup d'autres informations qui vont nous emmener vers un résolveur ou un autre endroit où je peux héberger mes informations, toutes mes données, mon nom, mon profil, mon Instagram, mon LinkedIn, mon Twitter et bien d'autres choses. C'est l'essence du programme.

À l'ENS, on a envisagé un monde où tout le monde peut utiliser leur domaine en tant qu'identificateur. Les domaines valides DNS qui ont un support DNSSEC, ce sont des domaines valides. Cela veut dire que vous pouvez avoir un contrat intelligent et soumettre votre DNS et fournir des faits probants disant que vous êtes propriétaire de tels domaines. Vous allez avoir des

validations. Et comme dans mon cas, vous pourrez dire : « Luc est en fait le propriétaire du nom de domaine luc.computer. » Et si je décide pour quelque raison de vendre luc.computer à une autre personne et que je fais les changements nécessaires vis-à-vis de mon bureau d'enregistrement, une autre personne pourra faire la même chose, aller voir vers les contrats intelligents et présenter les preuves nécessaires pour pouvoir faire transférer ce nom. Comme on l'a déjà dit, on fournit un registre sur la chaîne, c'est fait sur la chaîne et cela est disponible pour les utilisateurs de blockchain.

Par exemple, le .eth est le seul TLD que nous fournissons. Ce TLD nous permet de faire plus de choses que l'ICANN. Nous pouvons héberger des sites décentralisés, c'est une toute autre histoire. Ce sont des sites que les utilisateurs peuvent aller voir sur un serveur Web unique, plus de routine DNS, plus de localisation, plus d'utilisation de toutes ces infrastructures ; tout simplement héberger un site et tous les [inaudible] deviendront des caches par rapport aux autres utilisateurs. Là, nous parlons de quelque chose de complètement différent. En plus, les coûts d'enregistrement, bien sûr, préviendront le spam. Cela coûte très peu cher, c'est 5 $ par an. C'est un coût raisonnable. Cela vous donne beaucoup de contrôle et bien sûr, tout le monde ne va pas acheter énormément de sites Web.

Ces coûts vont directement à une organisation à but non lucratif qui s'appelle Dow. C'est une organisation autonome, décentralisée, une organisation qui est gérée un peu comme le modèle multipartite de l'ICANN. Nous sommes totalement transparents. Nous sommes gouvernés publiquement, nous avons des groupes de travail, nous faisons des propositions d'améliorations ENS. Nous sommes superviseur et bien sûr, n'importe qui peut participer.

Pourquoi ? Quelle est notre motivation derrière tout cela ? Nous sommes un collectif open source. Nous sommes des développeurs, des contributeurs qui veulent faire la différence dans le monde. Nous sommes financés par la fondation Dow d'ENS. Tous les ans, nous faisons des propositions, nous demandons tel ou tel montant d'argent pour les salaires à payer, pour les voyages, pour toutes sortes de dépenses que nous avons, le marketing, la comptabilité, etc. Et bien sûr, il y a un vote sur ces propositions et sur ce budget. Si nous, en tant que l'équipe de développement ENS, nous avons des conflits, le Dow se prononce et prend des décisions.

Au contraire des autres systèmes de nommage, comme on l'a déjà mentionné, nous avons un objectif : c'est d'étendre et d'améliorer la fonctionnalité du DNS pour aujourd'hui et pour demain.

Dans une minute, je pense après la prochaine présentation, nous aurons le temps pour des questions. Si vous avez des questions ou si votre question n'a pas de réponse ou si vous voulez me poser est une question plus tard, allez me voir sur luc.contact. Encore un autre nom de domaine.

Merci de votre temps.

ADIEL AKPLOGAN : Merci beaucoup. C'est une présentation très intéressante. Ce qui est intéressant, c'est l'utilisation de ce système de nommage alternatif qui est différent du DNS que l'on connaît aujourd'hui.

Maintenant, avant de passer à notre dernière intervention, je vais faire une pause et voir s'il y a des questions sur ces deux interventions qui sont liées l'une à l'autre. Nous allons passer aux questions avant de passer à l'intervention suivante. Y a-t-il des questions en ligne de la part des personnes qui sont avec nous en ligne ?

DAVID HUBERMAN : Oui, il y a une question en ligne, Adiel. Elle est adressée à Luc. Cette question est en deux parties : « .eth, est-ce qu'il y a des preuves du fonctionnement de la décentralisation pour l'utilisateur final ? Est-ce qu'il y a cet objectif de faire la distinction avec le DNS ? » La question est adressée à Luc.

LUC VAN KAMPEN : Tout d'abord, ce n'est pas lié à l'ENS mais au système Ethereum. Il y a le proof-of-work ou le proof-of-stake. Avec cette poussée de la communauté pour opérer des changements au réseau Ethereum, il y aura des améliorations en termes de frais, notamment, et tout cela, pour améliorer la vie des utilisateurs de l'ENS.

Comment l'intégration sera fluide ? Nous voyons des milliers de sites Web qui sont élaborés et il y a ces multiples applications qui vous permettent de vous connecter, comme cela a été dit. Il y a encore de nombreux problèmes, notamment l'intégration. Pour l'ENS, tant qu'il n'est pas intégré au niveau du DNS au niveau de la zone racine, il y aura la nécessité d'installer une extension, d'utiliser un navigateur compatible qui sera hébergé par nous-mêmes ou par la communauté.

J'espère avoir répondu à votre question.

ADIEL AKPLOGAN : Merci Luc.

Est-ce qu'il y a des questions dans la salle ?

BEN MCILWAIN : Bonjour. Au niveau de la nouvelle série de TLD, si quelqu'un faisait une demande différente, est-ce qu'il y aurait davantage de risques de collision ?

LUC VAN KAMPEN : Comme cela a été dit, la collision de noms, c'est une situation difficile. Il y a de nombreuses parties qui essayent d'enregistrer de nombreuses options qui ne fonctionnent pas avec notre philosophie. Le cas échéant, l'ICANN pourrait accorder des autorisations de noms qui nous porteraient préjudice, mais nous espérons que cela ne se produira pas. Nous essayons de faire en sorte que notre système demeure stable et opérationnel.

ADIEL AKPLOGAN : Si j'ai bien compris, vous allez faire une demande pour ce TLD ?

LUC VAN KAMPEN : Je ne peux pas répondre à cette question.

WARREN KUMARI : Conformément à notre guide, il y aurait des exigences auxquelles il faudrait répondre si vous souhaitez faire cette demande. Il y a ce guide de candidature. Il est tout à fait possible que nous mettions en place un service différent, car le système de nommage de l'ICANN a des exigences précises.

LUC VAN KAMPEN : Ce qui se passerait dans cette situation hypothétique, nous pourrions créer des services que les utilisateurs pourraient mettre en place. Si je m'enregistre et que je souhaite être disponible par le biais du DNS, il faudrait aller sur le site Web de l'ENS pour faire en sorte qu'il y ait conformité avec toutes les exigences de l'ICANN.

ADIEL AKPLOGAN : Merci.

John.

JOHN CRAIN : La technologie, c'est formidable, c'est intéressant, cela ne fait aucun doute. L'organisation ICANN pour laquelle je travaille discute de politique et de technologie. Je me demande, quels sont les garde-fous et quelles sont les normes que vous mettez en place pour gérer les mauvais comportements sur les menaces sécuritaires ?

LUC VAN KAMPEN : Dans la mise en œuvre actuelle de l'ENS et par rapport aux extensions, les domaines ne peuvent être révoqués ou éliminés. Cependant, si nous gérions une passerelle, nous pourrions alors

mettre cela en œuvre et nous pourrions aussi déterminer quels sont les informations qui sont disponibles conformément aux règles de l'ICANN.

JOHN CRAIN : Actuellement, si je suis un criminel, je m'enregistre, je suis actuellement toujours en sécurité, je ne perdrai pas mon nom.

LUC VAN KAMPEN : En vertu du système actuel, tout ce qui est dans le système ENS, tout ce qui est enregistré sous le nom .tld, c'est à l'abri de la censure.

ADIEL AKPLOGAN : Merci.

Nous passons maintenant à la présentation suivante. Si nous avons davantage de temps, nous passerons aux questions et réponses.

Maintenant, nous avons Jacques qui va prendre la parole sur l'identité numérique et les technologies émergentes en matière d'identificateurs.

JACQUES LATOUR : Bonjour à tous. Est-ce que vous pouvez m'entendre ? Bien. Je vais essayer d'être rapide.

Je m'appelle Jacques Latour, je suis chef de la technologie à CIRA, Autorité canadienne pour les enregistrements Internet. Je m'occupe de l'authentification au Canada, je travaille avec le laboratoire numérique du Canada. J'essaie de comprendre les défis auxquels nous sommes confrontés relatifs à la confiance. Voilà le sujet de mon intervention.

Dans le monde des émetteurs d'identités numériques, il y a les permis de conduire, par exemple, que l'on place dans son portefeuille. Je ne vais pas trop parler des portefeuilles et des nommages. Je veux parler de l'écosystème. Nous avons les émetteurs qui émettent des justificatifs d'identité vérifiable qui sont envoyés au portefeuille, comme votre permis de conduire physique, mais nos documents sont numériques. C'est ainsi que l'écosystème fonctionne. Tout est numérique, les gens peuvent présenter leur justificatif d'identité vérifiable. Il peut s'agir d'un permis de conduire, d'un diplôme universitaire, etc.

Prenons un cas de figure. Nous avons la CIRA. Nous avons un processus de vérification. Il faut vérifier la nationalité du titulaire. Est-ce qu'il est de nationalité canadienne ou est-ce qu'il est résident au Canada ? Actuellement, on reçoit une photocopie du passeport ou du justificatif et nous ne voulons pas cela. Dans le monde numérique, le gouvernement canadien émettrait un justificatif d'identité vérifiable, tels que le permis de conduire, le certificat de naissance ou autre. Ces documents sont signés par

l'émetteur du nom de domaine .ca qui est source de confiance au Canada. Ces justificatifs d'identité vérifiables sont signés, ils vont dans le portefeuille numérique et nous avons un vérificateur, la CIRA. Et nous, le titulaire, nous allons recueillir suffisamment d'informations pour prouver qu'il s'agit d'un ressortissant canadien ou d'un résident.

Maintenant, comment nous assurer que l'émetteur est digne de confiance ? Comment nous assurer qu'il s'agit véritablement d'un permis de conduire valable et non pas d'un faux ? Et comment le portefeuille est rempli de documents qui sont vérifiés ? Il faut que le passeport aille dans un certain portefeuille et le vérificateur, c'est la CIRA. Ce vérificateur a la possibilité de poser certaines questions.

Cet écosystème doit exister, il doit pouvoir être vérifiable. La réponse à toutes nos questions, c'est qu'il y ait un registre de confiance et nous pouvons alors vérifier que l'émetteur est authentique. Luc parlait de ces clés publiques du gouvernement canadien. Il y a une correspondance avec le registre. Avec cet agent de registre qui est .canada, les vérifications sont possibles. Le participant à ce système peut vérifier l'opérateur de registre et faire les vérifications nécessaires.

Le premier opérateur de registre de confiance actuellement est un répertoire, un référentiel qui entre dans un cadre. Un opérateur de registre de confiance, c'est par exemple le secteur

académique. Toutes les universités du Canada auraient par exemple une accréditation. Un opérateur de registre de confiance comprendrait toutes les entités qui peuvent y figurer. Par exemple, au Canada, il y aurait des centaines d'opérateurs de registre de confiance et c'est ce que l'on doit déterminer dans cette communauté. Est-ce que l'on peut en avoir des centaines ou des milliers ? Comment on peut savoir quels sont les opérateurs de registre de confiance au Canada ? Comment pouvez-vous déterminer qui ils sont, qui ils disent être ? Actuellement, il est difficile de savoir à quel opérateur de registre on peut faire confiance, car il manque les informations R et R.

Nous parlons maintenant des preuves d'identité uniques et des identifiants uniques. D'ailleurs, il n'y a pas d'identificateurs uniques. On a parlé déjà de cela lors des discussions. On peut voir que les personnes peuvent créer leur propre domaine, leur propre identité. Nous avons par exemple le gouvernement québécois dans une blockchain différente.

Il doit y avoir une structure d'identificateurs interopérable mondiale. Il faut qu'il y ait des accréditations, des justificatifs qui soient vérifiables. Il y en a maintenant, mais ils sont invérifiables.

Dans tout cela, je pense pour commencer, vous pourrez utiliser le DNS pour les émetteurs fondamentaux. Par exemple, pour les cartes d'identité, les permis de conduire, les passeports, etc., cela

pourrait être la base que nous pourrions utiliser pour ces noms de domaine.

Ensuite, nous pouvons tirer profit du DNSSEC que nous avons aujourd'hui. Cela nous permet d'avoir une chaîne de confiance depuis la racine. Nous pourrons ainsi avoir un DNS unique. Si nous avons un ancrage mondial que nous pouvons utiliser, nous pourrons en terminer avec une structure qui aura cet effet. Comme vous le voyez à l'écran, nous pourrons avoir… Attendez, je ne sais pas où j'en suis sur Zoom. Nous aurons donc un ancrage dans la zone racine et de là, nous aurons au sein de l'ICANN et de l'IANA un répertoire d'opérateurs de registre mondial par pays. Là, il y aura tous les TLD avec toutes les extensions géographiques. Là, nous aurons un opérateur de registre Canada Trust, Confiance Canada, et nous aurons ce que j'appelle les opérateurs de registre comme les universités, toutes les organisations, les associations qui doivent avoir leur propre écosystème. Chaque pays pourrait avoir ainsi sa propre structure. Nous pourrons faire la même chose du côté commercial. Cela fournirait une structure d'identificateurs uniques et c'est quelque chose qui manque pour l'instant. Quand les gens émettent des justificatifs sur une blockchain, il pourrait y avoir des blockchains différentes, des répertoires différents. Il faudrait aligner tout cela. Il y a la prolifération de blockchain et de ledgers, de répertoires qui rendent les identificateurs uniques non uniques. Ce n'est pas

pour les portefeuilles. Cela cible les émetteurs qui envoient des données pour que les portefeuilles puissent vérifier ces données.

À la fin du compte, avec le DNSSEC, nous devons construire ou bâtir des mécanismes pour trouver quels sont les opérateurs de registre de confiance pour pouvoir vérifier les émetteurs de données. Nous pourrons ainsi trouver des documents d'identification numérique qui viendront des noms de domaine. Le DNS est distribué et il peut être élargi. Ce serait la bonne plateforme pour cartographier tous les identificateurs d'une façon unique et d'une manière mondiale pour qu'il y ait une interopérabilité mondiale.

Au cours de la séance sur le DNSSEC tout à l'heure, il y a eu une présentation, il y a à peu près une heure ou deux, je ne sais plus, sur le DNSSEC. Elle était beaucoup plus technique et a fourni beaucoup plus de détails sur ce sujet.

ADIEL AKPLOGAN : Merci beaucoup, Jacques. Voilà un exemple de rassembler toutes les données d'identité dans le DNS. C'est complémentaire au sujet dont on a parlé tout à l'heure quand on parlait de l'utilisation du DNS.

Il nous reste encore quelques minutes. Je vais vous laisser un peu de temps pour que vous puissiez poser des questions au présentateur précédent.

GABRIEL KARSAN : J'ai une question. Je m'appelle Gabriel Karsan, je viens de Tanzanie et je suis boursier ICANN.

Ces technologies sont émergentes, mais pour nous, pour notre perspective du Sud global, je voudrais savoir quelle est la stratégie. Je vois qu'il y a beaucoup de confusion pour les utilisateurs. Nous venons de régions où les opérateurs n'ont pas beaucoup de ressources ou de connaissance sur le DNSSEC. Pour avoir l'accès à l'identité numérique, il faut avoir le DNSSEC, c'est obligatoire. Nous, dans notre région, nous n'avons pas la compréhension sur les Dow, sur la décentralisation, etc. Ce serait une bonne chose de pouvoir essayer d'enseigner, de passer les informations aux jeunes pour qu'ils puissent ainsi appliquer ces changements. C'est une façon plus démocratique de faire les choses.

Est-ce que vous êtes limités à des parties prenantes spécifiques ? Et comment est-ce que vous pourriez inclure la diversité et donc inclure les gens comme les gens qui viennent de ma région ? Merci.

LUC VAN KAMPEN : Il est important de noter qu'ENS Dow, la formation, le contrôle l'écosystème ENS, ceci veut dire que tout le monde peut participer. Il n'y a pas de pré-exigences, il n'y a pas de

discrimination dans ce sens, il n'y a pas de ce critère prédéfinis. Ceci veut dire que les contributions viennent des droits gouvernementaux. Il y a un petit pourcentage qui est donné aux cofondateurs. Il y a un grand pourcentage des marges qui est émis par le Dow. Si on veut travailler sur l'écosystème, le Dow doit voter sur tel ou tel projet. Nous avons une grande portion du financement qui est distribuée à travers les bureaux d'enregistrement.

En fait, ce qu'on a fait, c'est que toutes les personnes qui ont enregistré un domaine, nous leur avons livré des jetons, des allocations. Essentiellement, la distribution est faite vis-à-vis de la participation. Et bien sûr, tout le monde peut participer, il n'y a aucune discrimination, peu importe quel est votre pays, etc.

GABRIEL KARSAN : Pour avoir un compte, il faut que mon nom de domaine soit signé par le DNSSEC. Et si je suis dans un pays qui n'a pas encore signé le DNSSEC ou si je ne suis pas conforme au DNSSEC, j'ai donc besoin de m'engager à un niveau très bas. Donc, il faudrait inclure plus de personnes, des personnes qui n'ont pas accès à ces technologies émergentes.

LUC VAN KAMPEN : Merci de votre question. Ce que nous faisons, en fait, il s'agit de la distribution des fonds de la fondation. Si le domaine ne soutient

pas le DNSSEC, l'utilisateur peut enregistrer en ligne et il n'y a pas d'exigences. Si votre domaine n'est pas conforme au DNSSEC, parce que c'est un TLD qui n'est pas lié aux politiques de l'ICANN, cela veut dire qu'un utilisateur devrait s'enregistrer sous un autre TLD qui serait compatible au DNSSEC pour pouvoir utiliser le système ENS. Bien sûr, tout le monde peut participer aux technologies, mais au lieu de pouvoir choisir le domaine de leur choix, parce qu'ils n'en ont pas, ils auront un compte qui ne montrera que leur adresse.

Quand il s'agit de la sensibilisation, le Dow peut allouer un certain montant tous les ans pour tel ou tel programme et pour faire de la sensibilisation, encore une fois pour enseigner, pour faire de la formation. Nous essayons d'aller dans toutes les régions qui sont intéressées par ces technologies où nous pouvons offrir de l'aide. Bien sûr, je suis ici à l'événement Devcon qui aura lieu à Bogota en Colombie pour parler à la communauté locale. Nous voulons partager les informations qui viennent du réseau Ethereum et du Dow. Si vous avez plus de questions, vous pouvez me contacter.

ADIEL AKPLOGAN : Merci Luc. Tout cela est très intéressant.

Nous n'avons presque plus de temps. Habituellement, cette séance sur les identificateurs émergents est toujours une thématique très importante et très intéressante. Nous aimerions

tous vous encourager à vous renseigner parce que nous avons très peu de temps. Je ne pense pas que nous pouvons prendre plus de questions. Mais ce que je voulais faire, c'est que nous avons ce forum d'intérêt spécial en ligne. Si nous avons ce forum en ligne, c'est que nous pouvons ainsi continuer les conversations que nous avons durant les sessions de l'ICANN. Nous pouvons continuer ces conversations en ligne pour pouvoir vraiment continuer et en apprendre plus, approfondir le sujet au-delà de la durée d'une heure de cette session assignée à cette thématique ici durant la réunion.

Carlos, vous voulez prendre la parole ?

CARLOS ALVAREZ DEL PINO : Oui. Je voulais vous demander comment vous faites face aux demandes légitimes qui viennent des forces de l'ordre, par exemple pour les personnes qui enregistrent des noms de domaine.

ADIEL AKPLOGAN : Je pourrais vous demander de parler à Carlos après la séance parce que nous devons fermer cette réunion. Merci Carlos pour votre question.

Je sais qu’il y a d’autres questions dans le chat auxquelles nous devrons répondre sur la propriété intellectuelle, le squattage des noms et des questions sur l’ENS, etc.

Encore une fois, merci à tous. C’est une séance très informative. Je vous verrai plus tard. Vous pouvez bien sûr aller sur le Wiki de l’ICANN pour plus amples informations.

[FIN DE LA TRANSCRIPTION]