SelfKey

SelfKey Foundation

11 septembre 2017

Summaire

Problème : Vous n'êtes pas propriétaires de votre propre identité 3

Contexte 4

Limites d'un système d'identification centralisé 5

Sécurité et autres risques 5

Limitations d'accès 6

Monopoles 7

Conformité aux normes de protection des données 7

Exigences réglementaires « KYC » 8

Solution : Un écosystème d'identification numérique auto souverain « Selfkey » 10

Ecosystème d'identité 10

Comment fonctionne SelfKey pour un individu 13

Comment fonctionne SelfKey pour une entreprise 17

La fondation SelfKey 21

Les avantages du réseau SelfKey comparé aux systèmes d'identification traditionnels 25

Le jeton KEY 27

L'utilisation des jetons KEY 28

Un regard porté sur l'avenir 29

L'équipe SelfKey 32

Conclusion 32

Problème : Vous n'êtes pas propriétaires de votre propre identité

L'Internet s'est tellement répandu à travers le globe qu'il est maintenant devenu une réalité intrinsèque de la vie de tous les jours, quel que soit le domaine. L'Internet est un réseau numérique international technologique qui ne saurait être limité par les frontières traditionnelles. La transition du papier au traitement numérique et à l'Internet 1.0[i], puis 2.0[ii] compte parmi les plus grandes évolutions de l'histoire moderne. De nos jours, pratiquement tous les secteurs de l'activité humaine sont affectés par la numérisation, l'informatique et l'Internet. Nombreux sont ceux qui considèrent le développement de la blockchain comme un précurseur à l'Internet 3.0[iii]

Toutefois, en dépit des avancées technologiques et des bouleversements dans de nombreux domaines, les systèmes d'identification actuels fonctionnent avec des documents papiers émis par des entités gouvernementales en fonction de la nationalité et ne bénéficient pas des avantages offerts par l'Internet 3.0. En l'absence d'une infrastructure technologique moderne, des millions de gens dépendent - ou sont exclus - des systèmes d'identification traditionnels.[iv]

La plupart des systèmes sont planifiés et gérés selon un modèle centralisé, ne s'intègrent ou ne communiquent pas avec d'autres systèmes et n'accordent aucun droit au propriétaire de l'identité. Ces systèmes se soldent par des inefficacités, des fuites de données, des menaces, des violations de la vie privée et des vols d'identité[v] qui font que des milliards de personnes n'ont pas accès à des comptes financiers de quelque sorte que ce soit.[vi]

En outre, de nombreux systèmes d'identification centralisés sont affligés de problèmes de sécurité graves.[vii] La récente violation des données d'Equifax, qui pourrait avoir compromise les données personnelles de 143 million d'individus met en évidence la vulnérabilité des bases de données centralisées et remet en question la pratique qui consiste à réunir des collections centralisées de données extrêmement sensibles.[viii] Dans certains cas, tous les citoyens d'un pays (notamment la Suède[ix]) ont été victimes de violations de données personnelles au potentiel catastrophique. Ces violations de données ne se produisent souvent pas en raison d'un piratage

ou d'autres efforts malveillants, mais simplement en raison de l'absence de mesures préventives adéquates pour interdire l'accès non-autorisé aux données.[x]

Les systèmes d'identification actuels se sont avérés incapables de satisfaire aux exigences les plus élémentaires d'un système d'identification : sécurité, respect de la vie privée, propriété, accès, protection, interopérabilité ou portabilité des données pour les propriétaires des identités.

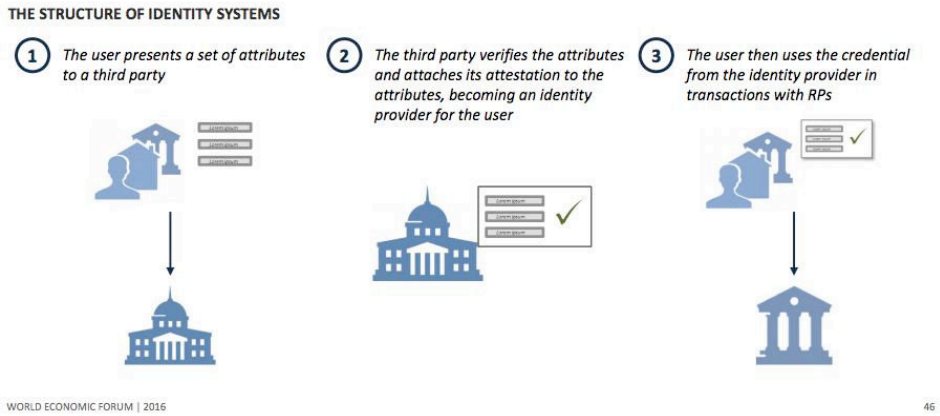
> « Les systèmes d'identification actuels limitent les innovations de Fintech ainsi que la mise en œuvre de services financiers efficaces et sécurisés, et les progrès de la société en général. L'identité numérique est largement reconnue comme l'étape suivante de l'évolution des systèmes d'identification. » – WEF[xi]

Les lacunes des systèmes d'identification centralisés traditionnels sont évidentes. Si l'on considère que les individus doivent rester propriétaires de leur identité face à la mondialisation de notre société, le développement d'un modèle d'identification numérique fiable est maintenant indispensable.

Contexte

Intervenants d'une transaction d'identité

Une transaction d'identification comprend habituellement trois intervenants : le propriétaire de l'identité (**IO** - par ex. un individu ou une entreprise), un garant de l'identité (**CI**) ou une tierce partie (un notaire ou un juge de paix) et un demandeur d'identité (**RP**), comme une banque, un courtier ou une autre institution financière). Le « IO » fait plusieurs déclarations d'identité (**IC**). Par exemple « Je m'appelle John H. Smith » ou « Je suis né le 1 janvier 1975 ». Ces déclarations sont validées ou vérifiées par une tierce partie, et l'IO peut ensuite partager ces déclarations validées avec un demandeur d'identité afin d'accéder à ses produits et services, notamment pour l'ouverture d'un compte bancaire.



À titre d'exemple, un individu (**IO**) souhaite prouver à un échange de cryptomonnaie (RP) qu'il est citoyen des États-Unis (**déclaration**) et qu'il dispose d'un passeport américain (**une preuve**) et que la copie numérique envoyée est une copie certifiée conforme de l'original. Cette déclaration d'identité électronique reçoit une **attestation**

d'un notaire et devient une **déclaration vérifiée.** Les déclarations vérifiées sont l'avenir de l'identité numérique.

Tous ces intervenants se débattent actuellement avec un système d'identification centralisé basé sur des documents papiers et pourraient grandement bénéficier d'un système d'identification numérique décentralisé.

Limites d'un système d'identification centralisé

Sécurité et autres risques

La plupart des systèmes d'identification disposent de bases de données centralisées contenant des millions voire des milliards de dossiers d'identité. En raison de leur taille colossale, ces bases de données centralisées sont des cibles de prédilection pour les pirates. Les données d'identification qu'elles contiennent sont relativement faciles à voler et à utiliser.[xii] Étant donné que les bénéfices d'une violation d'identité augmentent exponentiellement avec le nombre d'identités détenues dans la base de données, plus une base de base de données grandit, plus elle devient vulnérable à des attaques. En outre, l'existence d'une seule base de données gigantesque (par opposition à

de multiples bases de données décentralisées et segmentées) signifie généralement qu'un seul point de défaillance peut compromettre la totalité de la base de données.

Les systèmes d'identification centralisés sont habituellement gérés par un seul intervenant qui fait appel à des tierces parties pour accéder aux bases de données et traiter les données - souvent sans mesures de sécurité ou supervision adéquate - ce qui rend les bases de données d'autant plus vulnérables à des violations de données. Même si l'opérateur est digne de confiance, un système d'identification centralisé est à la merci des tierces parties qui disposent d'un accès autorisé. Les pièces d'identité des individus sont des biens précieux qui se vendent facilement sur le marché noir. Les acheteurs des informations d'identification volées peuvent commettre des fraudes ou d'autres crimes en utilisant les noms de propriétaires d'identité innocents. Au-delà des dégâts évidents causés au propriétaire de l'identité par les vols d'identité, ces violations de données exposent l'opérateur de la base de données centrale à des risques considérables.

Limitations d'accès

Les opérateurs limitent l'accès aux données afin de lutter contre les accès non autorisés à ces bases de données centralisées. Néanmoins, ces mesures empêchent souvent les propriétaires de ces identités d'accéder à leurs propres données.[xiii] Si les opérateurs ne permettent pas l'accès à ces données, celles-ci ne peuvent pas être reliées pour répondre aux besoins du propriétaire de l'identité.

Les données liées sont une composante essentielle d'une identité numérique[xiv], puisque c'est la liaison entre les données qui permet au propriétaire de l'identité de bénéficier de la création de relations entre leurs données.

La liaison des données ne présente aucune difficulté technologique. De fait, ces technologies sont déjà très répandues.

Les technologies clés nécessaires pour lier les données sont les URIs (une méthode pour identifier les entités) ; HTTP (un mécanisme simple mais universel pour l'accès aux ressources) ; et RDF (un modèle de données graphique générique qui permet d'organiser et de relier des données).[xv] Ces

technologies existent depuis des années mais les propriétaires des identités ne peuvent pas bénéficier de données liées.

Outre les limites techniques et les risques de sécurité liés à l'utilisation d'une base de données centralisée, l'existence d'une seule base de données massive contenant les identités présentent des problèmes pour l'entreprise qui la gère.

Monopoles

Si une seule organisation à but lucratif disposait d'une base de données contenant les informations d'identité de chaque personne sur la planète, elle pourrait agir en tant que monopole et facturer des prix exorbitants pour l'accès à ces données. En outre, si cette organisation parvenait à réunir suffisamment de données, l'« effet de réseau » créerait un effet de dépendance pour les utilisateurs. Les nouveaux intervenants sur le marché devraient faire face à des obstacles considérables. L'absence d'une concurrence efficace entraîne presqu'invariablement des tarifs monopolistes et entrave l'innovation.[xvi]

Conformité aux normes de protection des données

Une base de données massive centralisée des identités pourrait également contrevenir aux lois sur la protection des données et de la vie privée.

Les lois de protection des données nationales et supranationales sont conçues pour s'assurer que les gestionnaires des données mettent en œuvre des politiques et des procédures pour préserver la sécurité des données personnelles sous menace de lourdes sanctions monétaires voire d'emprisonnement. Toutefois, ces lois sont spécifiques à chaque juridiction et les normes de conformité varient considérablement. Au cours de ces dernières années, un nombre croissant de juridictions a adopté des mesures pour contrôler les exportations de données. À titre d'exemple, « l'union européenne considère que les lois sur la protection de la vie privée des États-Unis ne remplissent pas les exigences réglementaires européennes[xvii] ». Aussi, seules certaines entreprises seront autorisées à transférer des données de l'Europe vers les États-Unis, si elles se conforment au cadre juridique de « protection de la vie privée ». C'est un obstacle à l'entrée pour les nouvelles

startups qui ne peuvent pas faire face à des exigences réglementaires contraignantes aux coûts potentiellement très élevés. Qui plus est, le cadre juridique de « protection de la vie privée » est déjà remis en cause, seulement 18 mois après avoir remplacé le mécanisme de « sphère de sécurité » jugé insuffisant par la cour de justice de l'Union Européenne.

L'accord de l'utilisateur est au cœur de la plupart des lois sur la protection des données. Cet accord est normalement donné par les individus lorsqu'ils communiquent leurs données personnelles, en cochant une case ou par un autre mécanisme similaire. Toutefois, comme les individus ne sont pas au centre des processus de gestion des identités actuels, ils ne sont pas en mesure de donner (ou de révoquer) leur accord, bien que les lois en vigueur considèrent cette action comme un droit inaliénable. De plus en plus, la protection des données doit faire appel à des mécanismes de consentement dynamiques, mais ces derniers sont particulièrement difficiles à mettre en œuvre étant donné que les accords sont généralement sous forme papier.

Au cours de ces dernières années, les modes de partage des données à l'échelle internationale entre les autorités réglementaires de diverses juridictions, avec notamment l'introduction de FACTA, les normes de reporting communes et autres accords sur le partage international des données. Nombre de ces accords de partage sont aussi exempts des exigences de consentement dans le cadre des lois de protection de la vie privée nationale, et l'accord du propriétaire individuel n'est pas requis avant le partage de ses données. Le secteur financier, entre autres, transfère régulièrement des informations d'identification d'un pays à l'autre, et les données partagées entre les organismes de règlementation contiennent souvent des données d'identification obtenues dans le cadre du processus « KYC » (Connais ton client).

Exigences réglementaires « KYC »

Les lois qui gouvernent les procédures KYC s'appliquent aux juridictions nationales et internationales et concernent un ensemble varié de demandeurs d'identité, notamment (mais sans s'y limiter : échanges de cryptomonnaies, les startups Fintech, les sociétés de transfert de fonds, les entreprises et les agents immobiliers, les revendeurs et les services de dépôt de métaux

précieux, les fournisseurs de services aux entreprises, les préteurs, les banques, les sociétés de placement, les avocats, les comptables, les fondations à but non lucratif, les fournisseurs de service professionnels, les notaires, les gouvernements, les assurances, les réassureurs, les institutions financières, et d'une manière générale, toute entité légale ou personne naturelle qui gère de l'argent ou des services financiers.

KYC n'est pas optionnel - c'est une obligation et le non-respect des lois KYC peut entraîner des sanctions civiles et criminelles imposées par des organismes locaux et/ou internationaux. Malheureusement, pour de nombreux individus et entreprises - des petites startups aux grandes entreprises, ainsi que les demandeurs d'identité - la conformité KYC est une réalité douloureuse et onéreuse.

Pour les demandeurs d'identité - KYC est cher et demande beaucoup de temps. Le coût annuel moyen récurrent de la conformité KYC d'une banque typique est de 60M USD, mais peut se chiffrer jusqu'à 500M USD pour d'autres.[xviii] Ce coût est nécessairement élevé parce que les demandeurs d'identité ne peuvent pas accéder rapidement et simplement aux données d'identité mises à jour, valider les données ni les filtrer pour satisfaire aux exigences réglementaires. Aussi, les demandeurs d'identité doivent envoyer de nouvelles demandes au propriétaire de l'identité, traiter chaque propriétaire d'identité comme une « fiche vierge » et entreprendre une procédure KYC complète et fiable.

Le temps et l'effort passé par un des demandeurs de validation KYC ne peut être réutilisé ou recyclé et ne sert pas aux demandes futures. Si le propriétaire de l'identité décide de changer de prestataire de services, ces mêmes contrôles doivent être réalisés à nouveau par le nouveau demandeur d'identité. Les données d'identification ne sont pas « transmises » vers le nouveau prestataire de services et continuent donc à être détenues par différents prestataires pour des individus qui ne sont plus leurs clients, souvent de manière redondante, en dépit de la nature très sensible des données d'identification. Les frais élevés impliqués dans cette procédure constituent un obstacle à la sortie lors du changement de prestataire, ce qui se traduit par un environnement non compétitif, au détriment des propriétaires des identités, des startups Fintech et de l'innovation. D'une

manière générale, cette pratique augmente le risque de vol d'identité pour les individus.

En outre, ceux qui ne disposent pas de pièces d'identité émises par un gouvernement sont exclus entièrement des transactions commerciales, n'étant pas à même de se conformer aux règlements KYC. Les règlements KYC, aussi bien intentionnées soient-ils, n'en excluent pas moins des intervenants légitimes du marché[xix] et ralentissent les échanges commerciaux internationaux. Ce problème pourrait être résolu sans grande difficulté s'il existait un moyen de relier, réutiliser et transporter les données KYC d'un pays à l'autre tout en se conformant aux règlements en vigueur.

Solution : Un écosystème d'identification numérique auto souverain « Selfkey »

Ecosystème d'identité

Notre idée est simple : les utilisateurs doivent être au cœur de la gestion de leur identité, un concept connu sous le nom de **S**ystème auto-**S**ouverain d'**ID**entité (**SSID**). Nous pouvons nous libérer des systèmes papiers traditionnels et faire la transition vers une identité numérique capable de protéger la vie privée, la sécurité, la transparence et les droits des individus grâce à SelfKey, un système SSID basé sur la technologie blockchain, avec des clés correspondantes détenues dans un portefeuille numérique.

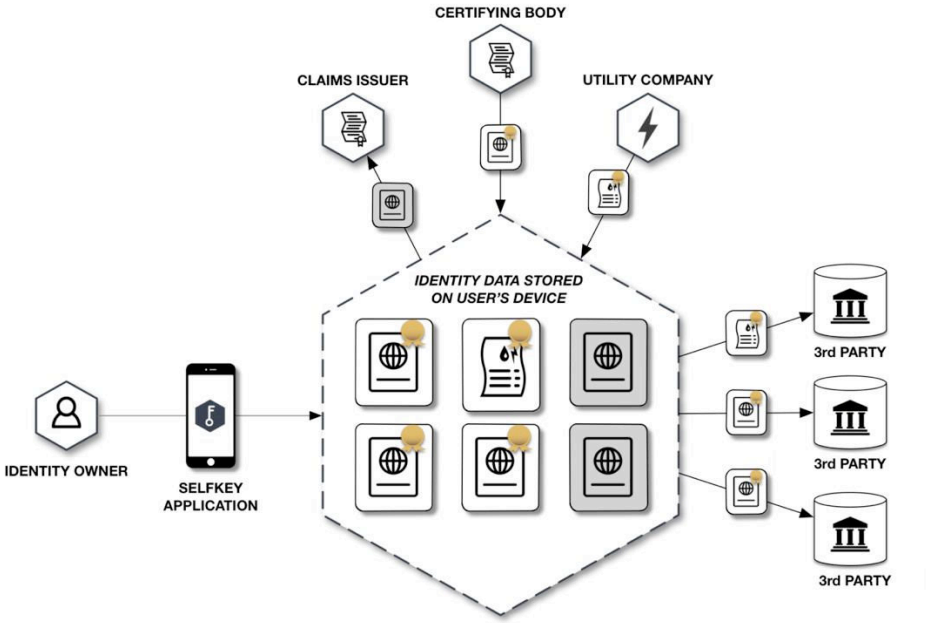
SelfKey est un système d'identification basé sur une plateforme ouverte composée de plusieurs éléments clés, notamment : **La fondation SelfKey, une organisation à but non lucratif** dont la charte et la gouvernance reflètent précisément les principes d'une identité auto souveraine, des technologies ouvertes et gratuites, avec notamment un **portefeuille gratuit et open source pour le propriétaire de l'identité**, un marché qui offre **des produits et des services réels** et disponibles dès le lancement, un protocole JSON-LD (lisible à la machine), une connexion à des micro-services d'identification de tierce partie conformes aux **lois et règlements KYC**, et **un jeton natif, le « KEY »,** qui permet à l'environnement SelfKey d'échanger des informations et des valeurs de manière efficace, numérique et auto-souveraine.

Les produits disponibles lors du lancement* comprennent :

- Inscriptions aux échanges d'actifs numériques, y compris pour le Bitcoin ;
- Programmes de citoyenneté par investissement ;
- Demandes de citoyenneté par investissement immobilier
- Création d'entreprise (notamment des sociétés en commandite par action, des fondations, de LLC, et des sociétés fiduciaires)
- Introduction et demande de compte bancaire
- Demande de permis de séjour dans plus de 50 pays
- Portefeuilles électroniques ou services de stockage de valeurs ;
- Achat et stockage d'or et de métaux précieux ;
- Demandes d'assurance internationale ;
- Services de transfert et de virement monétaire ;
- Vente de jetons

SelfKey est la solution aux limites des systèmes d'identification centralisés, avec un jeton KEY pour les propriétaires d'identité, les demandeurs et les vérificateurs, qui donne accès à des services pratiques réels. Grâce à SelfKey, il est maintenant possible de satisfaire les exigences les plus strictes en matière de KYC et de rendre au propriétaire de l'identité le contrôle de ses données personnelles.

Avec SelfKey, les transactions d'identification sont plus sûres, plus efficaces et respectent la vie privée tout en se conformant aux myriades de lois et de règlements actuellement en vigueur. SelfKey sert aussi à construire un monde meilleur, un monde où les systèmes d'identification sont centrés sur l'individu, dans lequel les identités sont vérifiées sur la base de signatures numériques, les données sont minimisées, les individus peuvent prouver leur identité et celle-ci est traitée selon les meilleures pratiques de gouvernance. Dans ce nouveau monde, l'utilisateur peut réellement contrôler, gérer et posséder son identité numérique. SelfKey est conçu pour être à l'épreuve de la censure, équitable, diversifié, agile et efficace grâce à un choix de technologies open source rationnel, une infrastructure et une gouvernance légale transparente au travers de la fondation SelfKey. SelfKey peut répondre aux besoins actuels et futurs des sociétés modernes et de l'Internet mondial en assurant que les droits de l'homme et les libertés fondamentales en matière d'identité soient respectés.



*Ces services ne sont pas disponibles dans les juridictions qui ne les autorisent pas. Ces services ne sont pas proposés directement par la fondation SelfKey mais par des partenaires qui acceptent les informations/données KYC fournies par les propriétaires des identités à l'aide de SelfKey.

Une solution grâce à la blockchain ?

Une blockchain est un registre distribué qui met les données à la disposition de tous les participants. Est-ce que nos données d'identité devraient **être stockées sur *et reproduites dans*** une blockchain contrôlée par plusieurs entités participantes (par exemple, les grandes banques ou les gouvernements) ?

Non. La blockchain en elle-même n'est pas une solution.

La reproduction de toutes les données d'identification, accessibles à tous les intervenants pourrait violer les lois sur la protection des données pour diverses raisons, et tout particulièrement l'exigence de conserver les données personnelles dans un territoire ou une juridiction spécifique. En outre, les règlements et les meilleures pratiques exigent que les entreprises ne retiennent que les données personnelles pertinentes à leur activités commerciales - et ce, uniquement avec la permission du client.

Les risques liés à la cybersécurité augmentent si les données d'identification sont reproduites dans tous les nœuds de blockchain. Comme nous l'avons vu précédemment, les entrepôts de données centralisés sont durs à sécuriser. Aussi, la simple utilisation d'une blockchain pour reproduire les données d'identification pour de nombreux intervenants forcerait chaque nœud de la chaîne à sécuriser correctement ces données. Et comme chaque organisation a ses propres pratiques (et lacunes) en matière de cybersécurité, un agresseur pourrait facilement mettre la main sur ces données. Même si les données personnelles sont chiffrées, le problème de la conformité juridique reste entier, parce que les données cryptées ne sont pas nécessairement autorisées par les lois sur la gestion des données personnelles.[xx] Une personne suffisamment motivée aurait probablement les moyens de réidentifier des individus en comparant les transactions sur le registre décentralisé et celles des autres bases de données disponibles. L'anonymat au sein de la blockchain ne suffit pas. À l'heure du « Big Data », les technologies d'analyse peuvent être utilisées pour comparer des bases de données apparemment dépourvues de données personnelles à des bases de données qui en contiennent et tenter de faire le rapprochement. C'est un défi juridique considérable pour les solutions blockchain qui enregistrent des données personnelles.

Existe-t'il une solution ?

Le concept d'une identité numérique auto souveraine ressemble à la façon dont nous enregistrons et gérons nos identités non numériques. Actuellement, la plupart d'entre nous gardons nos pièces d'identité, nos passeports, nos certificats de naissance, ou nos factures de services publics, etc. chez nous - en sureté, sous notre contrôle. Nous ne les partageons avec d'autres entités que lorsque nécessaire. Rares sont ceux qui confient ces documents vitaux (ou d'autres informations personnelles non requises) à une tierce partie - et cette situation nous convient tout à fait. L'identité auto-souveraine dans SelfKey est l'équivalent numérique de la façon dont nous gérons nos pièces d'identité physiques.

Comment fonctionne SelfKey pour un individu

Un nouvel utilisateur télécharge simplement l'application de portefeuille SelfKey sur un appareil personnel. Les données d'identification sont enregistrées localement, sur l'appareil. Un utilisateur a la possibilité de sauvegarder ces informations sur un autre appareil ou avec une solution de sauvegarde personnelle.

Lorsque l'utilisateur télécharge son portefeuille SelfKey, il est vide. La première chose qu'un utilisateur doit enregistrer dans le portefeuille est une paire de clés publique/privée (connue sous le nom de SelfKey). Cette SelfKey devient le « stylo » numérique de l'utilisateur qui peut être utilisé pour apposer la signature numérique unique du propriétaire de l'identité à des documents Parce que la clé privée n'est connue que du propriétaire de l'identité, dès que cette signature numérique est appliquée, elle permet d'authentifier et de valider l'identité du propriétaire auprès des demandeurs d'identité de manière confidentielle et sûre (sans nécessiter une présence physique).

SelfKey possède des avantages énormes par rapport à un nom d'utilisateur et un mot de passe classique. Chaque SelfKey est unique à son propriétaire. Alors qu'une combinaison nom d'utilisateur/mot de passe est enregistrée dans la base de données d'une tierce partie, un utilisateur SelfKey ne partage jamais sa clé privée, qui reste toujours secrète.

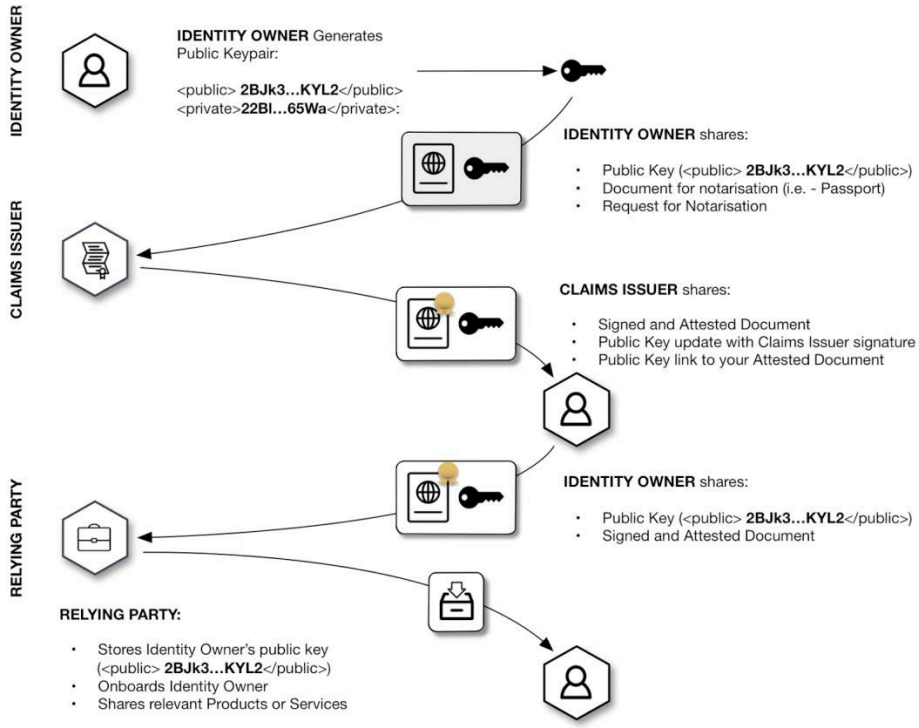
Personne - pas même la fondation SelfKey - n'a accès au contenu du portefeuille, ou peut même savoir que ce numéro SelfKey existe. Aucune autre entité ne l'a émise, et elle n'est créée que par l'utilisateur. C'est ce que l'on entend par « auto souverain ». L'utilisateur peut maintenant utiliser SelfKey avec des preuves d'identité pour recevoir des attestions des vérificateurs concernés, comme des notaires, des institutions gouvernementales, etc. Une fois que l'utilisateur a obtenu la validation de ses pièces d'identité dans son portefeuille numérique, il peut maintenant acheter des produits et des services sur le marché de SelfKey (comme expliqué ci-dessous).

Avant d'autoriser l'accès aux produits et services disponibles sur le marché SelfKey aux utilisateurs de SelfKey, ceux-ci doivent établir leur identité. Ces identités sont les attributs de l'utilisateur (ex. nationalité, date de naissance, profession, etc.) et sont enregistrés dans des zones de texte (blobs JSON-LD). Pour économiser

le temps nécessaire à la saisie manuelle des données, il est possible d'enregistrer des photos ou des numérisations de documents qui seront ensuite traitées par un logiciel de reconnaissance de caractère, ce qui simplifie grandement la procédure. Ces preuves d'identité ne sont nécessaires que pour satisfaire aux exigences KYC traditionnelles. À l'avenir, les attestions SelfKey signées numériquement permettront d'éliminer les pièces d'identité telles que nous les connaissons aujourd'hui.

Une fois que les déclarations d'identité ont été créées, l'étape suivante consiste à obtenir une attestation de ces déclarations. Ces attestations peuvent également être enregistrées dans le portefeuille SelfKey. Ces attestions sont des preuves d'identité lisibles en machine, signées numériquement et qui ne sont valides que pour une durée déterminée.

Les vérificateurs et/ou les autorités concernées, tels que les services publics, les notaires, les banques, les services des passeports, les hôpitaux, les services des permis de conduire, d'immigration, etc. ont la possibilité de signer et de valider les déclarations de l'utilisateur. Ces déclarations peuvent être signées de telle manière qu'une personne puisse révéler uniquement le minimum d'information. En d'autres termes, le demandeur d'identité n'aurait accès qu'aux informations qui lui sont strictement nécessaires, mais rien de plus.



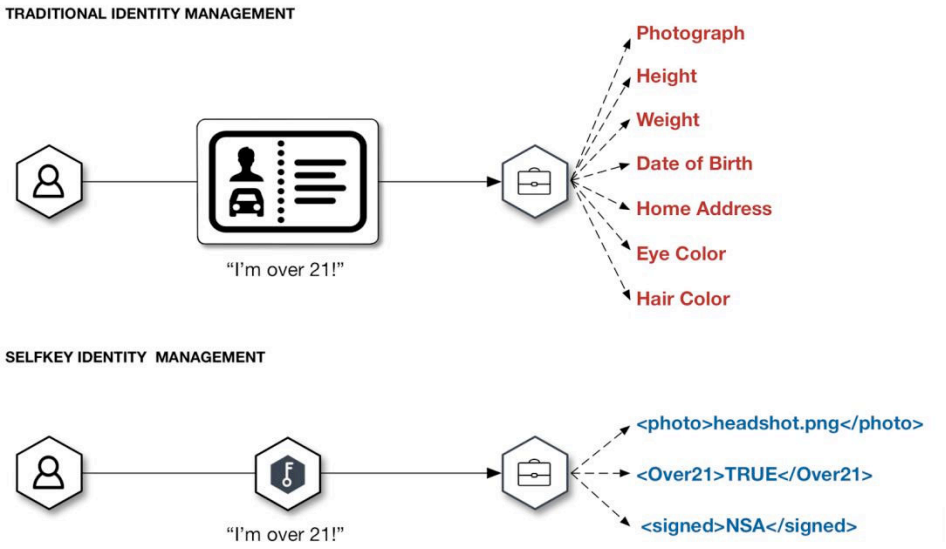
Par exemple, un utilisateur peut facilement prouver qu'il réside dans un certain pays. Ou prouver qu'il a plus de 18 ans, sans rien révéler d'autre que cette information. Les caractéristiques d'une identité sont sans limites et pourraient aussi inclure des informations telles que « investisseur professionnel ». Le propriétaire de l'identité aura la possibilité de choisir quelles sont les informations qu'il souhaite communiquer à un demandeur d'identité. Les types de déclaration d'identité qui peuvent être attestés sont virtuellement sans limite.

Les données sont enregistrées dans un appareil (sous le contrôle du propriétaire, comme les documents qu'il ou elle garde actuellement à la maison ou au bureau), et quand le propriétaire le souhaite, il ou elle a la possibilité d'autoriser une tierce partie à accéder à des données spécifiques. Cette autorisation peut être accordée en confirmant une notification sur l'appareil en question. Cette expérience est similaire à l'authentification par l'intermédiaire d'un compte Facebook.

L'analogie ne s'applique toutefois qu'à l'expérience utilisateur - au lieu de confier ses données personnelles aux serveurs de Facebook, un utilisateur pourra autoriser les demandes à partir de son propre stockage de données, tout en contrôlant exactement quelles données sont partagées. Contrairement

à bon nombre de sociétés Internet, la fondation SelfKey est une organisation à but non lucratif. Il n'y a aucune monétisation sous forme de publicité ou de vente des données des utilisateurs.

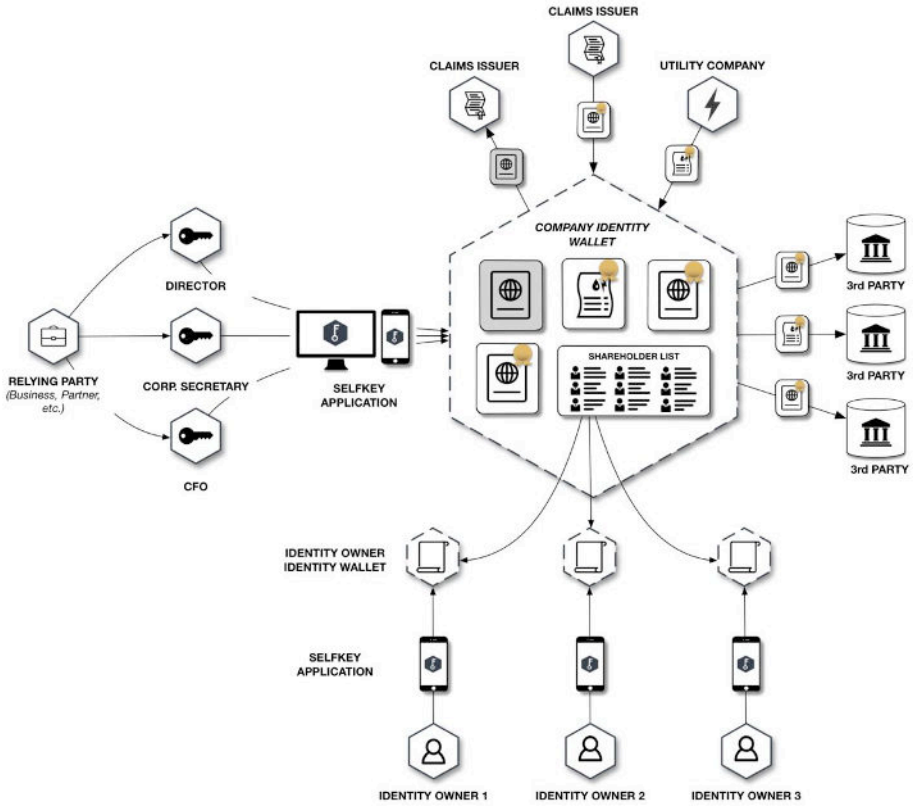
Minimiser la quantité de données à partager, c'est aussi minimiser les risques pour le propriétaire d'identité et pour le demandeur d'identité. Le propriétaire de l'identité ne partage pas des informations superflues ou sensibles, et le demandeur n'a pas besoin de les enregistrer. Ce système permet non seulement d'améliorer la sécurité, mais aussi la conformité aux lois locales sur la protection de la vie privée.



Comment fonctionne SelfKey pour une entreprise

Comme expliqué précédemment, les déclarations d'identité et les preuves vérifiées ne sont pas limitées à des individus mais peuvent également s'appliquer à des entreprises. Une entreprise peut tout aussi facilement gérer les documents de startup à partir du portefeuille d'identité. SelfKey possède les fonctions essentielles de gestion du tableau de la structure du capital et de gouvernance d'entreprise, ce qui permet à une entreprise de réaliser simplement des opérations habituellement fastidieuses, comme l'ouverture d'un compte bancaire. Lorsque les demandeurs d'identité intègrent une nouvelle entreprise, les procédures KYC doivent être réalisées non seulement au niveau de la société, mais aussi pour tous les actionnaires

majeurs à chaque niveau de participation au-dessus de l'entité, jusqu'à atteindre les propriétaires bénéficiaires finaux. Ce niveau de contrôle des documents est extrêmement fastidieux. En outre, la procédure KYC électronique est particulièrement attrayante pour les nombreuses sociétés dotées de multiples filiales ou concessions dans plusieurs pays, si les identités liées facilitent le contrôle sur plusieurs niveaux, un problème insoluble avec un système centralisé national. Grâce à SelfKey, les sociétés peuvent facilement prouver des états de fait qui sont habituellement très difficiles à prouver pour les propriétaires d'identité et à valider pour les demandeurs d'identité (plusieurs niveaux de participation au capital, structures complexes, structures de capitaux en évolution permanente).



Comment fonctionne SelfKey pour un vérificateur

Un grand nombre d'entreprises et d'institutions dans le monde entier émettent (ou pourraient émettre) des attestions pour le compte des propriétaires d'identité à l'usage des demandeurs d'identité. Les exemples les plus courant dans le cadre de la KYC sont les services publics (qui

émettent actuellement des documents imprimés), les banques (qui fournissent des lettres d'attestation) et les registres des entreprises (qui émettent des documents imprimés). SelfKey peut aujourd'hui être utilisé pour numériser et monétiser ces déclarations d'identité que les demandeurs d'identité sont prêts à payer. Cette procédure renforce la cryptoéconomie dans l'écosystème SelfKey. Les vérificateurs peuvent aussi émettre directement un certificat numérique sur la plateforme SelfKey. Les propriétaires de cette entreprise pourraient attester de ce fait instantanément en prouvant qu'ils possèdent les SelfKeys utilisées pour enregistrer les actions.[xxi]

Le réseau SelfKey

Le réseau SelfKey va au-delà d'un simple système d'identification pour le partage sur l'Internet en P2P anonyme et sécurisé de données structurées et de fichiers. Le réseau SelfKey se distingue par plusieurs caractéristiques novatrices afin de favoriser son adoption et sa réussite à long terme. Ces caractéristiques sont présentées plus en détail ci-dessous.

Fondation

Comme expliqué précédemment, aucune entreprise ne peut à elle-seule contrôler ou administrer un système d'identification. Aussi, une fondation a été créée non pas pour contrôler le réseau, mais pour en préserver certains principes constitutionnels (décrits ci-dessous). La fondation protège et préserve les principes fondateurs de l'identité auto souveraine.

Organisation à but non lucratif

La mission première de la fondation SelfKey est d'assurer la réussite du réseau dans son ensemble et du jeton (KEY) qui permet de gérer les transactions du réseau. La fondation est une organisation à but non lucratif implantée à l'île Maurice et bénéficie d'un « bac à sable » réglementaire (sandbox) conçu permettre aux entreprises technologiques spécialisées dans la blockchain de développer et de commercialiser leurs applications. La fondation SelfKey ne commercialise pas les données d'identité qui transitent dans ses systèmes, que ce soit par la vente ou la publicité. La valeur transite sur le réseau uniquement sous forme de jetons KEY natifs.

Le jeton ERC-20 « KEY » est au cœur du réseau SelfKey. KEY est un acronyme anglais signifiant « Clé d'auto encryptage » (Key to Encrypt Yourself). Ce jeton peut être utilisé pour accéder à des produits et des services sur le réseau. À titre d'exemple, le KEY est indispensable pour participer. Il est utilisé pour encourager la participation, un comportement acceptable et créer une cryptoéconomie auto-alimentée pour la gestion de l'identité susceptible d'apprécier au fur et à mesure que les individus et les entreprises rejoignent le réseau, ce qui augmente la demande de la KEY. Certaines actions sur le réseau ne pourront se faire que grâce à un échange de KEY, et d'autres actions nécessiteront le placement de KEY dans un contrat scellé (pour accéder au réseau et éviter le spam causé par les attaques Sybil). L'existence d'un mécanisme POI (Preuve d'individualité) peut avoir des ramifications considérables sur le réseau Ethereum

Gouvernance

SelfKey a été fondée par une entreprise commerciale, KYC-Chain Ltd. (KYCC) qui a publié le code sous licence open source et réalisé la contribution monétaire nécessaire pour établir la fondation. KYCC peut continuer à développer des logiciels pour la fondation, mais la réussite du réseau SelfKey repose également sur les contributions des détenteurs de jetons KEY à la plateforme open source. L'adhésion ne donne pas de droit à un dividende ou à une quelconque distribution des profits de la fondation SelfKey. Les détenteurs de jetons KEY ne doivent pas anticiper de profits dérivés de l'acquisition de jetons KEY, bien qu'ils soient susceptibles d'obtenir des récompenses financières pour leurs contributions à la croissance du réseau.

Cadre juridique

La conformité aux lois et règlements existants sur la protection et la confidentialité des données, et autres dispositions légales y afférant est un objectif majeur de tout système d'identification aspirant à atteindre la masse critique en vue d'une adoption généralisée. Aussi, l'architecture SelfKey est conçue pour être aussi décentralisée que possible, accessible dans le monde entier et conforme aux réglementations, tout particulièrement à l'égard des lois sur la confidentialité des données. Cette conformité est accomplie grâce

à une approche souple basée sur l'utilisateur, qui ne force pas l'utilisateur à stocker ses documents dans un système de stockage spécifique et qui sollicite l'autorisation du propriétaire de l'identité avant de procéder à toute transaction d'identification.

Les propriétaires des identités contrôlent à tout instant leur identité, les demandeurs d'identité peuvent recevoir rapidement les déclarations d'identité, et les vérificateurs peuvent recevoir des paiements pour leurs contributions et attestations. Cette architecture souple centrée sur l'utilisateur est conforme aux exigences de nombreux pays en matière de transfert de données vers l'étranger.

Étant donné qu'un système d'identification peut évoluer et changer en raison de contraintes légales et ou technologiques - l'organisation fera preuve d'une certaine adaptabilité à certains égards (par exemple, un hachage de la couche de stockage pourrait être ajouté à la blockchain à titre d'horodatage), mais restera inflexible à d'autres, en particulier la préservation des droits individuels et de l'identité auto souveraine. La constitution de la fondation SelfKey est basée sur les principes suivants :

La fondation SelfKey

Ces principes de constitution sont intrinsèques aux mécanismes de contrôle et de gouvernance de la fondation SelfKey. Toute infraction à ces principes serait contraire à la constitution, ce qui donne à ces principes une valeur juridiquement contraignante.

Existence. Les utilisateurs conservent toujours une existence indépendante. Toute identité auto souveraine dérive d'une preuve d'existence. Afin de garantir que l'individu reste au cœur de de SelfKey, notre système est conçu pour exister en dehors des frontières d'un quelconque système national, et au lieu de donner priorité à une nation, le participant principal de notre système est un individu, une personne physique vivante.

Contrôle Les utilisateurs conservent le contrôle complet de leurs identités. L'utilisateur est l'autorité ultime au sujet de sa propre identité. Les utilisateurs peuvent faire référence à leur identité, la mettre à jour, voire

même la cacher ou la faire disparaitre. Les utilisateurs peuvent opter pour une identité publique ou privée dans leurs préférences individuelles.

Accès Les utilisateurs ont accès à leurs propres données. Ils peuvent facilement accéder à toutes les déclarations et autres données. En d'autres termes, le réseau ne permet pas de conserver de données cachées sur un utilisateur. Cela ne signifie pas qu'un utilisateur peut modifier une déclaration à sa seule discrétion, mais les utilisateurs sont conscients de toute déclaration concernant leur identité.

Transparence. Les systèmes et les algorithmes de SelfKey sont transparents et open source, aussi bien dans leur fonctionnement que dans la façon dont ils sont gérés et mis à jour. La fondation qui gère le système est aussi transparente.

Durabilité Les identités sont durables. Les clés privées peuvent être perdues ou remplacées, et les données peuvent être changées, mais l'identité elle-même demeure.

Portabilité Toutes les informations seront transportables et ne seront pas détenues par une seule tierce partie, le propriétaire de l'identité gardant le contrôle son identité.

Consentement Les propriétaires doivent approuver tous les transferts et toutes utilisations de leurs données.

Minimisation Les données relatives aux demandes doivent être minimisées. Les données fournies en réponse à une demande d'identification doivent être réduites au strict minimum nécessaire pour satisfaire à la demande. Le minimum d'informations utilisateur est communiqué aux entités correctes lorsque les circonstances le justifient.

Protection. En cas de conflit entre les besoins du réseau d'identité et les droits des utilisateurs individuels, le réseau SelfKey préservera les libertés et les droits des individus en priorité par rapport aux besoins du réseau. La validation de l'identité sera effectuée par le biais d'algorithmes indépendants décentralisés à l'abris de toute censure ou de toute attaque de force brute.

Interopérabilité L'interopérabilité est un objectif majeur de SelfKey. La résistance inhérente à la censure de la blockchain, l'autonomie des clés privées et publiques et l'identité souveraine permet l'utilisation du système dans de nombreuses industries. Des efforts sont faits pour assurer l'interopérabilité avec d'autres systèmes d'identification.

Ces principes font partie intégrante de la constitution de la fondation et les membres du conseil d'administration élus par les membres ne peuvent passer une résolution ou une action que si celle-ci est compatible avec ces principes.

L'environnement technologique SelfKey

Nœuds de validation- Notre système est basé sur des nœuds Ethereum utilisés à des fins de validation. Nous avons considéré l'utilisation de la « preuve d'autorité » Ethereum à ce niveau, mais nous avons opté pour le mécanisme de consensus normal d'Ethereum qui pourra être changé en cas de problèmes. Nous avons effectué des essais basés sur les protocoles de consensus de EVM, Eris, Monax et Tendermint, et des blockchains alternatives pourront être utilisées par la suite si le conseil d'administration de la fondation juge cette mesure nécessaire. Selon nos recherches, une blockchain publique existante largement reconnue serait la solution la plus équitable et la plus inclusive.

Couche Blockchain - Les paires de clés SelfKey proviennent du réseau public Ethereum.

Stockage - Compte tenu des défis de conformité avec les systèmes d'identification mondiaux, nous avons laissé la couche de stockage à la discrétion du propriétaire de l'identité. Les documents résideront localement sur l'appareil de l'utilisateur à moins que celui-ci ne décide (à sa discrétion) de déplacer les documents ou les données. Par la suite, des pilotes de stockage seront créés pour aider l'utilisateur à contrôler le stockage.

Gestion/récupération des clés

Dans un système d'identification blockchain géré par l'utilisateur, on peut

s'attendre à ce que certains utilisateurs perdent ou égarent leurs clés. En l'absence d'un mécanisme pour récupérer la clé, toutes les attestations seraient perdues. Heureusement nous avons développé une solution. SelfKey prévoit d'utiliser Uport, un mécanisme de récupération de clé convivial, grâce auquel un utilisateur peut récupérer un ou plusieurs comptes de son choix. Uport permettra l'interopérabilité selon des normes déjà acceptées par la communauté Ethereum.

The proxy contract Solidity code is very simple, and is presented here for reference:

```
contract Owned {
    address public owner;
    modifier onlyOwner(){ if (isOwner(msg.sender)) _ }
    modifier ifOwner(address sender) { if(isOwner(sender)) _ }

    function Owned(){
        owner = msg.sender;
    }

    function isOwner(address addr) public returns(bool) { return addr == owner;
}

    function transfer(address _owner) onlyOwner {
        owner = _owner;
    }
}

contract Proxy is Owned {
    event Forwarded (address indexed destination,uint value,bytes data);

    function forward(address destination, uint value, bytes data) onlyOwner {
        if (!destination.call.value(value)(data)) {throw;}
        Forwarded(destination, value, data);
    }
}
```

Protocoles-Afin de maximiser l'interopérabilité du réseau SelfKey, la couche des protocoles fera l'objet d'une amélioration continue ainsi que de plusieurs normes. Cette couche défini comment les données seront transférés d'un endroit à l'autre sous forme structurée (éventuellement d'une blockchain à une autre). Des recherches sont faites dans ce domaine pour développer l'interopérabilité avec les autres systèmes d'identification majeurs : Sovrin, W3C, Uport, etc.

Portefeuille d'identité - Le portefeuille d'identité SelfKey sera disponible au lancement et sera le point de départ de toutes les transactions d'identification. Le portefeuille servira également à stocker KEY.

L'utilisateur peut aussi accéder à différentes applications de la couche d'application grâce au portefeuille d'identité. Toute entreprise peut produire des applications pour cette couche. Tout fournisseur d'identité peut rendre

ses clés ou certificats interopérables, notamment les divers certificats x509 éligibles dans le cadre d'une ordonnance de transaction électronique gouvernementale arbitraire.

Micro-services d'identification - La couche des micro-services servira essentiellement à la conformité avec les lois et règlements internationaux, et sera utilisée essentiellement par les vérificateurs et les demandeurs d'identification. Toute entreprise peut fournir ces micro-services, mais afin de prendre en charge dès le début la couche d'application et plusieurs ICO qui utiliserons le système SelfKey, KYCC a construit et mis en œuvre plusieurs micro-services, notamment le filtrage par liste de sanction (remédiateur), la fonction de recherche sur le registre des entreprises, et la collection & validation des documents (collecteur).

Couche d'application - Toute sorte d'applications peuvent être créées sur la plateforme SelfKey, grâce à des APIs et du code open source, y compris un portefeuille entièrement open source.

Les avantages du réseau SelfKey comparé aux systèmes d'identification traditionnels

Un écosystème d'identification présente de nombreux avantages pour tous les intervenants, qu'il s'agisse des propriétaires des identités, des demandeurs d'identification et des vérificateurs, qui ont chacun leurs propres priorités. Le graphique ci-dessous explique pourquoi un système d'identification décentralisé peut profiter à tous les intervenants.

Systèmes d'identification centralisés traditionnels	**Système d'identification décentralisé SelfKey**
Propriétaires des identités	
-ne possèdent pas et ne contrôlent pas leurs identités -doivent effectuer à multiples reprises les processus d'accueil pour se conformer aux règlements -doivent garder plusieurs dispositifs	-ont un contrôle absolu de leur identité et doivent donner leur accord -authentification pour plusieurs services avec une seule paire de clés enregistrées dans un portefeuille

d'authentification à portée de main pour se connecter -ne peuvent pas transférer facilement les informations d'un service à un autre (coûts de transfert élevés) -doivent partager des pièces d'identité et ne peuvent pas partager le minimum d'informations -n'existent pour les demandeurs d'identité que sous la permission et l'autorité d'un gouvernement -ne peuvent pas réutiliser/recycler les résultats d'un contrôle d'identité ou d'une procédure KYC -la gestion des documents de l'entreprise est complexe et il est difficile de réunir les signatures nécessaires aux décisions importantes.	-peuvent partager le minimum d'informations -peuvent récupérer une clé perdue -peuvent accéder à un marché de produits fintech et de services d'identification -peuvent signer des documents et parvenir à un consensus de l'entreprise
Vérificateurs	
-ne peuvent pas monétiser les déclarations d'identité (ex. : services publics) -ne peuvent pas révoquer les déclarations -ne peuvent pas attester rapidement aux déclarations -les déclarations d'identité sont parfois frauduleuses	-peuvent monétiser les déclarations d'identité grâce au KEY -peuvent révoquer les déclarations -peuvent attester rapidement aux déclarations -les déclarations émises sont plus fiables
Demandeurs d'identification	
-doivent effectuer des efforts considérables pour accueillir les clients tout en se conformant aux exigences réglementaires -ont des procédures d'accueil pénibles qui agacent leurs clients -ne peuvent pas importer les données des clients	-peuvent rapidement accueillir les propriétaires des identités -peuvent créer une expérience positive pour leurs clients -peuvent facilement demander des détails supplémentaires aux clients -peuvent bénéficier d'économies

-doivent dépenser des sommes considérables pour valider la KYC -conformité internationale couteuse et difficile compliant -les procédures sont basées sur des documents papier et des efforts manuels des équipes de conformité	d'échelle -peuvent se conformer aux règlements internationaux -les procédures sont centrées sur KEY et vérifiées par les Demandeurs d'identification
Fonctions et avantages généraux	
-de grandes quantités de données sont stockées dans un silo -bénéfices énormes pour les pirates informatiques et donc une plus grande cible -propriétaire et opaque -aucune valeur retournée à l'utilisateur -possédé et contrôlé par une seule partie -un point de défaillance unique -a entraîné de par le passé des pertes de données massives, des fraudes et limite le progrès vers une gestion numérique auto souveraine de l'identité	-un réseau distribué qui permet de nombreux stockages de petite aillet -moindres bénéfices en cas de pénétration -centré sur l'utilisateur -Open Source -aucun point de défaillance unique -aucun contrôle/gestion centralisé -plus approprié à un contexte international -plus transparent

Le jeton KEY

Le jeton KEY jouera un rôle critique dans l'écosystème parce que tous les produits et services seront disponibles grâce à un système de payement en KEY, qui permettra de gérer l'« écosystème d'identité » de diverses manières. Par exemple, le KEY peut être utilisé pour payer les demandes d'attestations ; recevoir les déclarations d'identité (et rémunérer les utilisateurs) ; payer pour les annonces sur le marché ; et d'une manière générale, échanger des valeurs, encourager l'utilisation, l'adoption et donner accès au système.

Comme le montre le diagramme ci-dessous, chaque membre de l'écosystème

joue un rôle important dans l'adoption du système, l'utilisation de KEY, les attestations d'identité et des déclarations. Ce diagramme ne constitue pas une liste complète des utilisations de KEY - mais il devrait être évident qu'il existe un nombre d'utilisations considérable pour le jeton dès le lancement du réseau, et contrairement à de nombreux autres jetons, le KEY possède une valeur intrinsèque.

L'utilisation des jetons KEY

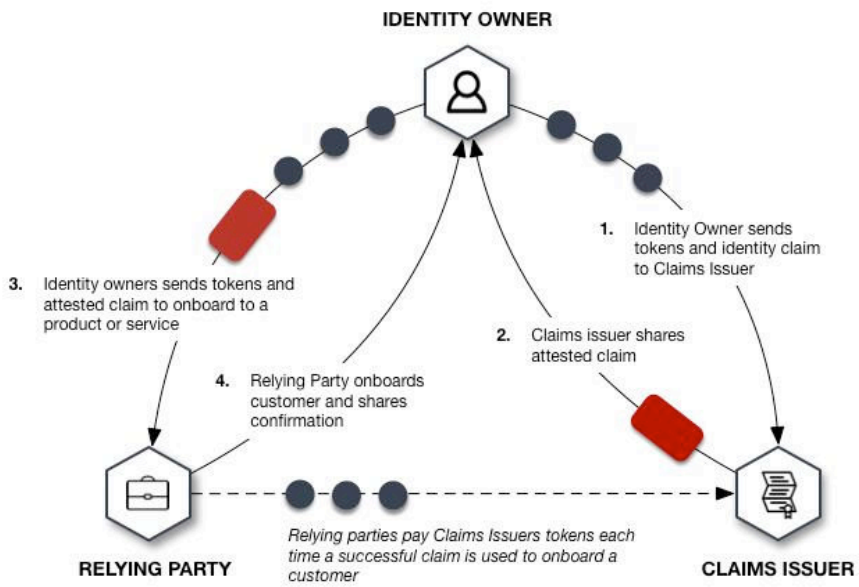
Les services suivants seront disponibles lors du lancement du réseau SelfKey :

- Inscriptions aux échanges d'actifs numériques, y compris pour le Bitcoin
- Programmes de citoyenneté par investissement
- Demandes de citoyenneté par investissement immobilier
- Création d'entreprise (notamment des sociétés en commandite par action, des fondations, de LLC, et des sociétés fiduciaires)
- Introduction et demande de compte bancaire
- Demande de permis de séjour dans plus de 50 pays
- Portefeuilles électroniques ou services de stockage de valeurs ;
- Achat et stockage d'or et de métaux précieux ;
- Demandes d'assurance internationale
- Services de transfert et de virement monétaire ;
- Vente de jetons

Dans cet écosystème, seuls trois intervenants échangent des valeurs Les propriétaires d'identité, les demandeurs d'identité et les vérificateurs.

SelfKey disposera d'un cadre de confiance qui sera signé par les demandeurs d'identité, les propriétaires des identités et les vérificateurs. Le concept de « contrat de confiance » n'est pas nouveau. « Les contrats de confiance sont souvent utilisés dans le domaine de l'identification, numérique ou non. Ils sont généralement utilisés pour contrôler une variété de systèmes multipartites où les intervenants souhaitent effectuer un type de transaction commun avec n'importe lequel des autres intervenants, de manière cohérente et prévisible. Ils fonctionnent bien dans ce contexte et peuvent s'adapter à grande échelle. »[xxii]

Le contrat de confiance SelfKey contiendra des informations sur le protocole, mais également des informations sur KEY afin d'encourager des comportements positifs. Les propriétaires d'identité, les vérificateurs et les demandeurs d'identité devront signer ce contrat de confiance qui encourage la bonne utilisation du réseau. Ces documents seront publiés à l'approche du lancement public du réseau et tiendront compte des remarques de la communauté.



Un regard porté sur l'avenir

Notre hypothèse de travail est qu'il est très difficile de développer un système conforme à toutes les lois sur la protection de la vie privée de chaque juridiction. Aussi, le propriétaire de l'identité contrôle le stockage de ses données et toutes les actions sont effectuées par le propriétaire de l'identité.

En outre, les données personnelles et les données d'identification ne sont pas conservées dans les registres des transactions, mais sont remplacées par une référence chiffrée aux données - un « hachage ». Les hachages, ou « empreintes » aident le propriétaire de l'identité à prouver que les données existaient à une certaine date, mais sans partager la déclaration d'identité - les données sur la chaîne sont totalement anonymes et brouillées.

L'utilisation de hachages tient compte du fait que la technologie blockchain est conçue pour conserver un registre permanent inchangeable de toutes les transactions réalisées, ce qui fait que, dans le contexte de la blockchain, le « droit d'être oublié » est impossible. Les lois sur la protection des données du monde entier exigent que les données personnelles ne soient conservées que tant que les données sont requises. Nous sommes convaincus qu'un hachage limitant l'accès aux données personnelles dans la blockchain est une solution viable pour se conformer aux exigences de protection des données. Certes, les données personnelles chiffrées peuvent être classées comme des données personnelles dans certaines juridictions tant que le propriétaire dispose de la clé de chiffrage. Toutefois, si l'on peut prouver que les clés ne sont communiquées que lorsque l'individu le souhaite, les exigences de protection des données devraient être remplies.

Les données sont transférées d'un endroit à l'autre par HTTPS, et des développements sont en cours sur les protocoles de messages P2P anonyme et sur les méthodes de chiffrage pairwise pour le transfert des données. D'une manière générale, un utilisateur peut être assuré que : 1. Les données ne sont transférées qu'avec son accord. 2. La protection des données passe en premier et que les données ne sont jamais partagées par la fondation. 3. Chaque transaction d'identité est chiffrée. 4. Les données ne transitent pas par la blockchain, à proprement parler. Le transfert se produit en dehors de la blockchain par le biais de protocoles chiffrés de données structurées et de messagerie.

La blockchain contient un hachage des données, ce qui permet de prouver que les données n'ont pas été changées. Ce mécanisme d'horodatage est d'une importance capitale pour prouver que les documents sont à jour. Des mesures seront prises pour éviter la corrélation des données et les risques de violations de la vie privée qui en découlent.

Portefeuille SelfKey

Le portefeuille (qui permet à l'utilisateur d'enregistrer et de gérer les détails de son identité et ses déclarations) est disponible en open source sous

Windows, Mac et Linux. Ce portefeuille sera porté vers les plateformes mobiles conformément à la stratégie de produits de SelfKey.

Écosystème SelfKey

L'écosystème d'identification SelfKey est un autre aspect de la plateforme sur lequel nous travaillons. SelfKey comprend trois intervenants primaires : 1) les propriétaires des identités ; 2) les demandeurs d'identification ; et 3) les vérificateurs (ou les auteurs de la déclaration). SelfKey engagera donc une stratégie de marketing à trois niveaux pour réunir ces trois types d'intervenants sur le réseau.

Marché SelfKey

Le marché est une composante clé de l'écosystème SelfKey parce qu'il permet aux propriétaires de l'identité de voir quels demandeurs d'identification utilisent actuellement le système SelfKey. Sur le marché, les propriétaires d'identité peuvent consulter diverses offres de produits financiers et commander certains produits. Les demandeurs d'identification et les prestataires de services peuvent publier des offres gratuites ou payantes sur le marché. Comme le marché est bilatéral, KEY peut être utilisé comme jeton principal ou comme une ressource pour échanger des valeurs.

Minimisation des données SelfKey

La minimisation des données, ou en d'autres termes, des fragments d'identité, constitue un aspect majeur du système. Elle permet au propriétaire de l'identité de fournir le minimum d'informations possible pour répondre aux exigences du demandeur d'identification ou du vérificateur. Cet objectif peut être réalisé grâce à une technologie avancée comme les preuves sans communication d'information (ZKP), mais il peut aussi être réalisé à l'aide de protocoles spécifiques ou de fragments d'identité. Une personne pourrait, par exemple, prouver qu'elle réside à Singapour sans révéler son adresse exacte. Cela peut être réalisé grâce à une planification adéquate des données sans exiger le développement prolongé lié aux ZKPs. Une partie des fonds levés par la campagne de financement sera dédiée à la minimisation des données.

Preuve d'individualité SelfKey (recherche biométrique)

Comme SelfKey se base sur l'existence d'une personne vivante, un élément

clé du projet SelfKey est que l'identité d'une personne ne *commence* pas avec une pièce d'identité émise par le gouvernement, mais avec une personne vivante. À cette fin, une certaine quantité de recherche sera engagée sur la Preuve d'Individualité (POI) de telle sorte que toute personne, où que ce soit dans le monde, puisse prouver son existence à un moment donné, et obtenir l'accès au réseau SelfKey. Un autre livre blanc est consacré à ce processus et sera publié lors la validation de la POI et du passage en phase de test. Selon nous, la POI peut être traitée de manière plus fiable grâce à la biométrique que par les solutions actuellement proposées par la communauté Ethereum

- une série de conférences vidéo. En outre, la fondation financera le développement d'un mécanisme de récupération des clés perdues selon des procédures strictement biométriques, de telle sorte que si vous perdiez vos clés, vous n'auriez pas besoin d'un mot de passe complexe, juste de votre corps.

L'équipe SelfKey

L'équipe de projet SelfKey est composée d'innovateurs expérimentés et passionnés par l'identité et son futur, d'entrepreneurs chevronnés et d'experts juridiques brillants. Consultez www.SelfKey.org pour plus de détails.

Conclusion

Selon SelfKey, l'évolution globale de notre société demande une nouvelle approche de l'identification, un système d'identification auto souverain. SelfKey est un système de gestion et de récupération de clé distribué, comprenant un protocole pour la préservation de la vie privée basé sur des déclarations vérifiées conformes aux normes W3C, dans un format compatible JSON-LD, une blockchain puissante entièrement décentralisée et développé par une fondation à but non lucratif dont la gouvernance est distribuée. Le Temple d'Apollon à Delphes construit il y a 3000 ans porte

l'inscription : γν ῶθισεαυτόν ; « Connais-toi toi-même ». Aujourd'hui comme autrefois, il ne fait aucun doute que vous êtes la personne la plus qualifié pour gérer votre propre identité. Alors que nous entrons dans un

monde de plus en plus numérique, nos vies deviendront de plus en plus intégrées à l'infrastructure de l'Internet public. Nos identités numériques sont menacées et ne sont actuellement pas sous le contrôle de leurs propriétaires légitimes.

La gestion d'une identité auto-souveraine sur des clés blockchain ne représente qu'une partie de la solution, mais avec ce livre blanc, la fondation SelfKey propose un écosystème, une technologie, une gouvernance et un cadre juridique qui vous permettrait de vraiment posséder votre propre identité.

[i] "What is web 1.0?" *Technopedia*. Accessed August 3, 2017, https://www.technopedia.com/definition/27960/web-10.

ii "Instead of merely reading a Web 2.0 site, a user is invited to contribute to the site's content by commenting on published articles or creating a user account or profile on the site…The unique aspect of this migration… is that customers are building… business(es) for [corporations]," Quotation from article entitled "Web 2.0," *Wikipedia,* accessed August 3, 2017, https://en.wikipedia.org/wiki/web_2.0.

iii Rob Marvin, "Blockchain: The Invisible Technology That's Changing the World," *PCMag*, published August 2, 2017,https://www.pcmag.com/article/351486/blockchain-the-invisible-technology-thats-changing-the-wor.

See Also:

Adam tinworth, "Next16: Blockchain Will Build Web 3.0, Says Jamie Burke," *Next Conference*, Published September 23, 2016, https://nextconf.eu/2016/09/next16-blockchain-will-build-web-3-0-says-jamie-burke/.

Sirikiat Bunworaset, "Web 3.0: Ethereum Will Change Everything," *Bangkok Post*, Published June 20, 2017, http://www.bangkokpost.com/business/news/1272219/web-3-0-ethereum-will-change-everything.

Los Silva, "Web 3.0: How Decentralized Applications Are Changing Online Censorship," *Ethnews*, Published February 5, 2017, https://www.ethnews.com/web-30-how-decentralized-applications-are-changing-online-censorship.

Tristan Winters, "Web 3.0 – A Chat With Ethereum's Gavin Wood," *Bitcoin magazine,* Published April 25, 2014, https://bitcoinmagazine.com/articles/web-3-0-chat-ethereums-gavin-wood-1398455401/.

"The Blockchain the New Web 3.0," Accessed August 3, 2017, https://www.moneyoip.com/new-web-3-0.

iv "The right to an identity – the global situation," *Humanium,* Accessed August 3, 2017, http://www.humanium.org/en/world/right-to-identity/.

v Jean Camp, "Identity in Digital Government: A report of the 2003 Civic Scenario Workshop," (An Event of the Kennedy School of Government, Harvard University, Cambridge, MA, 02138, April 28, 2002) http://www.ljean.com/files/identity.pdf.

vi Ben Schiller, "2 Billion People Are Still Left Out Of The Modern Financial System: How Quickly Can We Change That?," *Fast Company,* Published November 3, 2015, https://www.fastcompany.com/3051846/2-billion-people-are-still-left-out-of-the-modern-financial-system-how-quickly-can-we-change.

vii Ravi Raja Konathala, "What are the privacy issues with Aadhaar?", *Quora* (question-and-answer forum), April 5, 2017, https://www.quora.com/what-are-the-privacy-issues-with-aadhaar.

viii Equifax shares drop as questions mount over data breach https://www.ft.com/content/f503ef3c-94b2-11e7-a9e6-11d2f0ebb7f0

ix Tech2 News Staff, "Massive Swedish data breach reveals Swedish military secrets and the identity of almost all its citizens," *Tech2*, Published July 26, 2017, http://www.firstpost.com/tech/news-analysis/massive-swedish-data-breach-leaks-swedish-military-secrets-and-the-identity-of-almost-all-its-citizens-3855113.html

xi "A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity," *World Economic Forum*, Published in August 2016, http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf.

xii "Data Breach Tracker: All the Major Companies That Have Been Hacked," *Time*, Published October 30, 2014, http://time.com/money/3528487/data-breach-identity-theft-jp-morgan-kmart-staples/.

xiii

xiv Ambrose McNevin, "The five biggest issues in identity management and what's behind them," *Computers Business Review*, Published May 20, 2016, http://www.cbronline.com/news/cloud/the-top-five-issues-in-identity-management-4899761/.

xv SEE SUBHEADING "KYC-CHAIN" UNDER HEADING "USE CASES:", *UN-BLOCKCHAIN,* https://un-blockchain.org/use-cases/identity-under-construction/.

xvi WIKIPEDIA CONTRIBUTORS, "SEMANTIC WEB," WIKIPEDIA, THE FREE ENCYCLOPEDIA, ACCESSED AUGUST 3, 2017, HTTPS://EN.WIKIPEDIA.ORG/W/INDEX.PHP?TITLE=SEMANTIC_WEB&OLDID=793179594.

xvii NITASHA TIKU, "DIGITAL PRIVACY IS MAKING ANTITRUST EXCITING AGAIN," *WIRED*, PUBLISHED JUNE 4, 2017, https://www.wired.com/2017/06/ntitrust-watchdogs-eye-big-techs-monopoly-data/.

xvii "BLOCKCHAINS AND LAWS. ARE THEY COMPATIBLE?", *BAKER MCKENZIE* IN COLLABORATION WITH *R3*, ACCESSED AUGUST 3, 2017, http://www.bakermckenzie.com/en/-/media/files/expertise/fig/br_fig_blockchainsandlaws_jul17.pdf.

19 "THOMSON REUTERS 2016 KNOW YOUR CUSTOMER SURVEYS REVEAL ESCALATING COSTS AND COMPLEXITY," PRESS RELEASE, *THOMSON REUTERS,* PUBLISHED MAY 09, 2016, https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html.

xix GABRIELLA JÓŹWIAK "KYC LEADS TO FINANCIAL EXCLUSION", *THE GUARDIAN*, PUBLISHED FEBRUARY 2015.

xx NIGEL CORY, "CROSS BORDER DATA FLOWS WHERE ARE THE BARRIERS AND WHAT DO THEY COST?", *ITIF*, PUBLISHED MAY 7, 2017, HTTPS://ITIF.ORG/PUBLICATIONS/2017/05/01/CROSS-BORDER-DATA-FLOWS-WHERE-ARE-BARRIERS-AND-WHAT-DO-THEY-COST MAY 1, 2017.

xxi "REGTECH FOR KNOW-YOUR-CUSTOMER PROCEDURES: ENABLING & OPERATING ON BLOCKCHAIN TECHNOLOGY," PUBLISHED 2016, HTTP://WWW.SEC.OR.TH/FINTECH/DOCUMENTS/KYC.PDF.

xxii HTTP://WWW.OPENIDENTITYEXCHANGE.ORG/BLOG/2017/06/22/TRUST-FRAMEWORKS-FOR-IDENTITY-SYSTEMS-2/