Business Case
Projet KYChaine

Groupe GBC160 :

BUFFO Lucas
DEPRESLE Théo
LAVIRON Aurélien

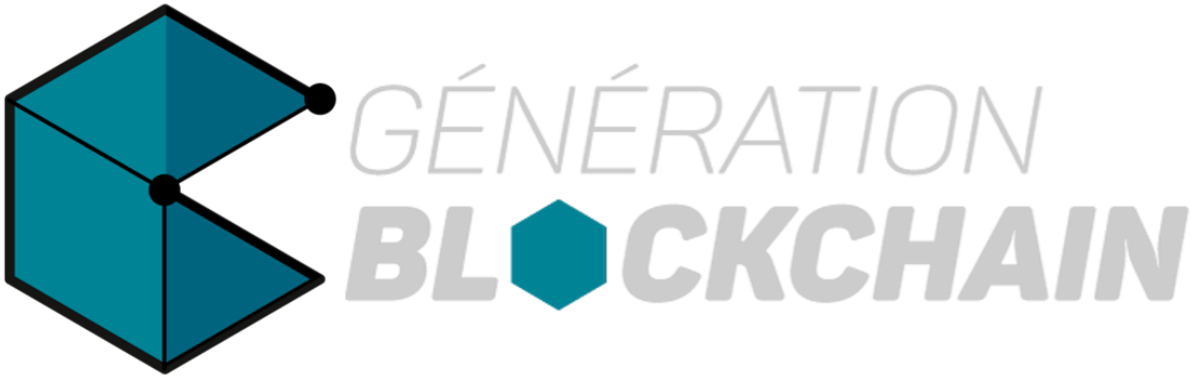


Table des matières

1. Contexte - Identification et description du besoin et des défis

Dans notre société, nous faisons face quotidiennement au besoin de partager des informations personnelles aux personnes et entreprises qui nous entourent. Le processus utilisé actuellement n'est pas optimal. Chaque personne stocke personnellement, de manière numérique ou non, tous les papiers officiels dont elle a besoin, et que des tiers peuvent lui demander afin de prouver une situation ou d'établir un contrat.

Pour chaque nouveau service auquel on adhère, nous sommes obligés de fournir nom, prénom, adresse, date de naissance, justificatif de domicile, et beaucoup d'autres justificatifs administratifs, allant des fiches de paie, au casier judiciaire, en passant par divers contrats passés avec d'autres organismes au préalable.

Afin de faciliter ces démarches rébarbatives, une idée en discussion au gouvernement est de centraliser toutes les données des personnes et de donner accès à certaines de ces données aux organismes qui en ont besoin, avec l'accord de l'utilisateur. Une sorte de portefeuille électronique, une identité numérique unique et censée être privée.

Mais un problème survient, une personne, ici l'Etat, possède les données de toutes les personnes enregistrées, et cela soulève de nombreux problèmes d'éthiques. Les données peuvent être détournées par une personne mal intentionnée qui a accès à cette base centrale. Un second problème est le stockage de ces données sensibles. Si cette base centrale est compromise, toutes les données seront accessibles et pourront être rendues publiques, ce qui peut nuire à toute la population.

Notre idée d'innovation s'inscrit dans le "Know Your Customer", abrégé "KYC". C'est la vérification de l'identité du client par un fournisseur de services. Ce processus est réglementé internationalement et obligatoire pour tout établissement bancaire. Les défis en jeu sont la lutte contre l'usurpation d'identité, le blanchiment d'argent, la corruption ainsi que les conflits d'intérêt. C'est un processus actuel lourd, puisqu'il faut récolter beaucoup de données sur le client et les vérifier. Nous souhaitons proposer une solution efficace en rupture avec un traitement individuel et encore très souvent manuel, permettant d'établir un contrat de confiance infalsifiable entre tous les acteurs du marché.

Le processus de KYC est simple :

- Collecter les données client.
- Vérifier la cohérence de ces données, et vérifier la non-présence du client sur des listes dans les pays concernés (personnes politiquement exposées, criminels, terroristes...).
- Évaluer le risque associé au client (embargo internationaux, exposition aux médias et à la politique. Réputation, historique voir méthodes de management de l'entreprise).
- Analyse du comportement et des transactions tout au long du contrat.

Ce secteur est nouveau, et de nombreux problèmes d'éthiques, de responsabilité freinent l'émergence de solutions qui permettraient de répondre à un besoin commun.

2. Description fonctionnelle de la solution, schéma et explications

Nous souhaitons mettre en place un service universel, simple d'utilisation, sécurisé et uniformisé afin de permettre aux utilisateurs de gérer une identité numérique, et de contrôler l'accès donné à des tiers sur celle-ci.

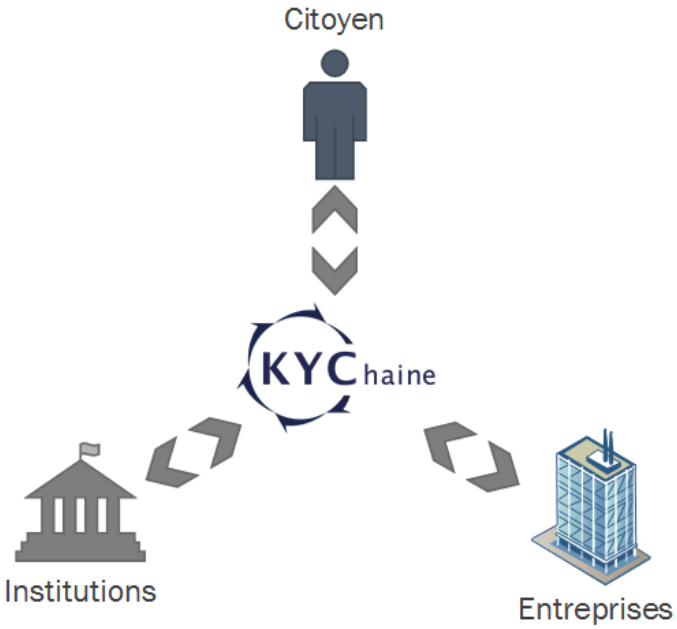
Nous avons pensé à un service qui décentraliserait les données afin qu'il n'existe plus d'accès universel à l'ensemble des informations. La blockchain permet ceci, et bien plus encore. L'ensemble

des données est public mais cryptée et seul l'utilisateur dispose des clefs permettant d'accéder aux informations.

Chaque utilisateur dispose d'une adresse qui va correspondre à son identité. Chaque information stockée dans la blockchain lui est rattachée. On sait ainsi à tout moment, à qui appartient une information et par qui elle a été déposée.

Certains services d'état disposeront également d'une signature et pourront authentifier certaines informations concernant un utilisateur. On pense notamment à l'état civil permettant de s'assurer de la véracité d'une identité ou encore le ministère de la justice concernant les inscriptions de peines dans un casier judiciaire.

L'utilisateur possède une signature qu'il acquiert à la naissance. Cette clé peut être cryptée en fonction de son empreinte digitale combiné avec d'autres paramètres afin de rendre la clé absolument unique. En cas de perte, l'utilisateur pourrait donc retrouver ses informations sans que cette information de cryptage ne soit stockée et soit ainsi vulnérable.



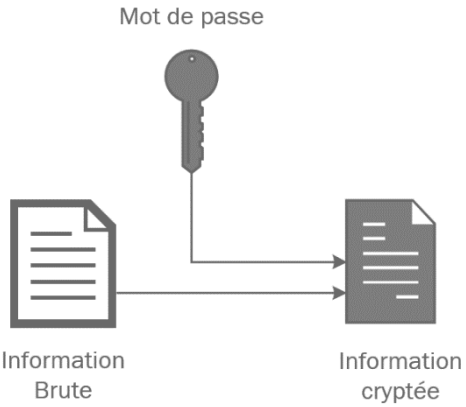
a. Stockage des données

Notre infrastructure pourra stocker toutes sortes d'informations relevant du KYC. L'utilisation d'une blockchain garantit l'authenticité des données en se prémunissant contre l'usurpation d'identité et la modification d'une information après sa publication. Une information publiée pourra donc être tracée, sa source authentifiée et son contenu garanti. Afin de garantir au maximum la confidentialité des données stockées tout en autorisant leur partage, nous avons mis en place une combinaison de cryptographie symétrique et asymétrique.

La cryptographie symétrique est la forme la plus répandue : on dispose d'un mot de passe permettant de crypter une donnée. Il est ensuite possible de la décrypter avec ce même mot de passe.

La cryptographie asymétrique utilise deux éléments de sécurité. Deux clefs sont utilisées. L'une crypte l'information et demeure publique afin que tout le monde puisse l'utiliser. L'autre est dite privée ; elle, et elle seule peut décrypter l'information. Elle sera détenue exclusivement par son propriétaire qui ne doit pas la partager.

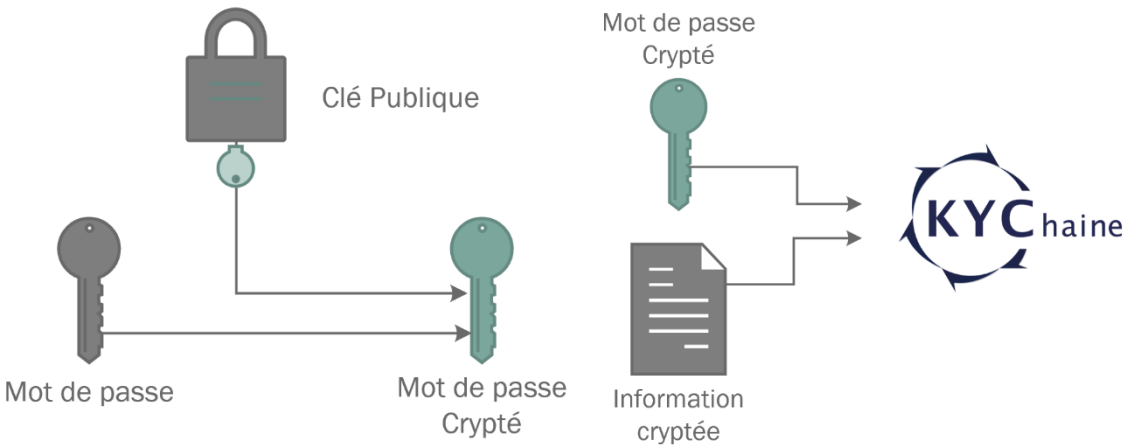
Dans le processus de stockage que nous employons, une entité (entreprise ou organisme public) souhaite publier une information sur un citoyen.



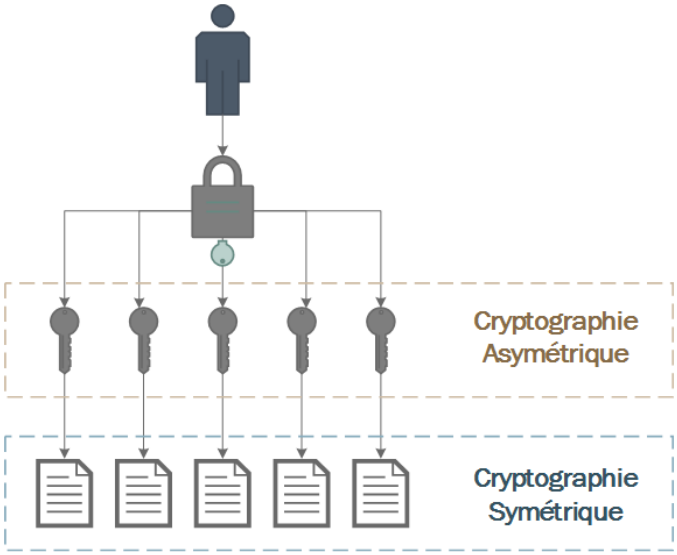
Dans un premier temps, l'information brute de l'utilisateur est encryptée à l'aide d'un mot de passe généré aléatoirement. L'information devient donc illisible à toute personne ne disposant pas du mot de passe. Une fois cryptée, cette donnée est inscrite sur la blockchain.

Par la suite, l'entité émettrice de l'information souhaite fournir de manière confidentielle le mot de passe permettant d'accéder à l'information de l'utilisateur. C'est ici que la cryptographie asymétrique entre en jeu.

Chaque utilisateur et entité dispose d'un couple de clés de cryptographie asymétrique. La clef publique est publiée dans un registre libre d'accès sur la blockchain. L'entité accède à ce registre et récupère la clef publique de l'utilisateur. Elle va l'utiliser pour crypter le mot de passe de manière à ce que seul l'utilisateur final puisse y accéder.

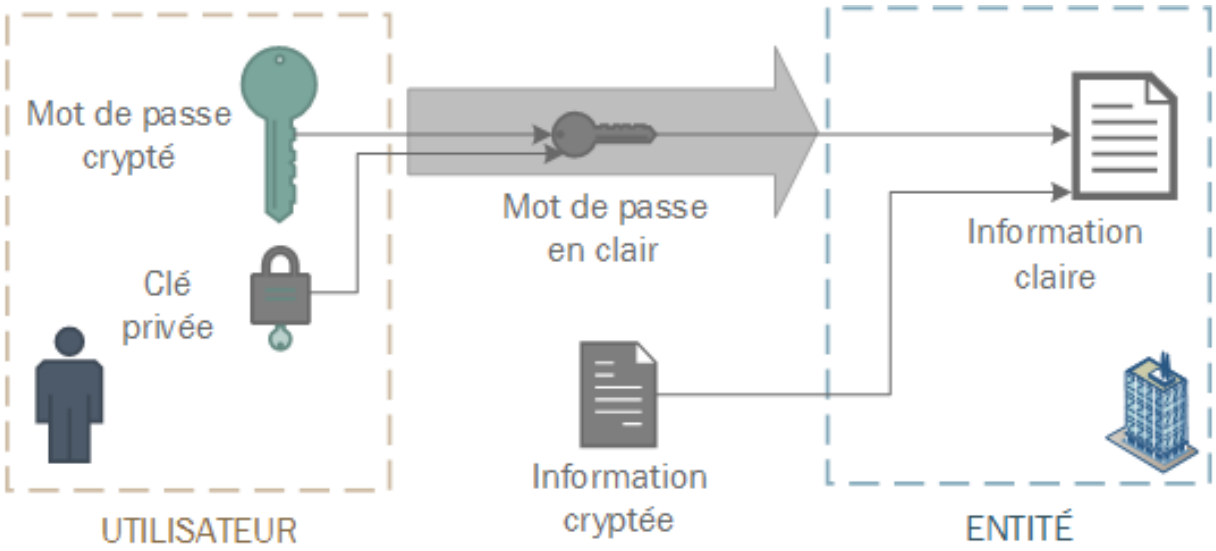


Une fois encryptées, ces deux informations peuvent être déposées sur la blockchain. Les données sont protégées par une sécurité à deux niveaux. Désormais, l'utilisateur peut accéder à la donnée le concernant en décryptant le mot de passe à l'aide de sa clé privée. Il pourra ensuite décrypter l'information en utilisant ce mot de passe.



Ce procédé permet à l'utilisateur de lire ses données, mais également de les partager de manière atomique. Il peut ainsi transmettre à une autre entité une seule information sans exposer ni compromettre les autres.

Pour transmettre une information à une entité, l'utilisateur va décrypter le mot de passe puis lui communiquer. L'entité pourra ensuite utiliser le mot de passe pour accéder à l'information.



Afin de simplifier ce processus d'ajout et de partage de données pour les utilisateurs, une interface va permettre d'automatiser tous ces traitements. L'utilisateur utilisera sa clef privée pour décrypter les messages et notre service se chargera de réaliser les transferts de données. Ceci rend alors facilement réalisable le transfert de groupe de données vers une entité lors de l'ouverture d'un compte bancaire ou de la signature d'un bail.

Il est important de noter que l'utilisateur reste le seul possesseur de cette clef. Elle ne transite à aucun moment sur nos serveurs.

Ce chapitre résume de manière simplifié les traitements et les échanges autour de la blockchain. D'avantages d'informations techniques sont disponibles dans la partie Spécifications techniques à la fin de ce document.

3. Avantages et argumentaire d'utilisation d'une Blockchain

Les avantages par rapport aux autres solutions sont nombreux. Ceux-ci permettent de comprendre toute l'ampleur du projet, et les répercussions directes sur le traitement des dossiers des clients pour les entreprises, ainsi que les répercussions pour chacun, de permettre un contrôle de ses données personnelles, chose qui est aujourd'hui compliqué.

Voici une liste non exhaustive des avantages de cette technologie, par rapport à la méthode actuelle, mais aussi par rapport aux autres solutions concurrentielles :

- Cette technologie facilite les démarches administratives. On peut facilement donner accès à une information pour un établissement donné.
- Cela apporte de la sécurité au document. Etant donné qu'on donne accès au même document, tout le monde vérifie la véracité de celui-ci, et aucune modification peut être faite à posteriori par une tierce personne dessus.
- Cela réduit le temps de traitement des dossiers, la perte des documents et les dossiers incomplets. Cela forcera aussi les personnes à garder informatiquement les données et favorisera la copie numérique plutôt que l'impression papier.
- L'utilisateur aura le contrôle total sur toutes ses données et personne d'autre.
- L'utilisateur donnera une permission individuelle à chaque organisme pour accéder à ses informations et choisi exactement les données qu'il veut transmettre.
- A terme, cela favorisera les "Smart Contracts" et la standardisation des données. Les entreprises auront les mêmes types de contrats et de données, pour un traitement plus efficace.

La technologie du blockchain face aux autres solutions est vraiment efficace. Le KYC (Know Your Customer) est un principe largement appliqué qui comporte beaucoup de points faibles, que le blockchain peut contrecarrer. Voici les problématiques actuelles et comment le blockchain peut les résoudre :

- KYC est actuellement un principe coûteux, peu efficace, lent et sensible au vol de données.
- KYC est un processus qui prend du temps et n'est pas en soi une entrée d'argent pour l'entreprise. C'est plutôt une garantie sur le long terme qu'il n'y ait pas de mauvaises surprises compte tenu de la nature du client.
- Le Blockchain sécurise les transactions. Celles-ci sont impossibles à supprimer et donc aucune donnée inscrite ne peut jamais manquer à un dossier futur.
- Les données sont partagées : tout le monde accède au même document. Si le document est actualisé, il l'est pour tout le monde en même temps.
- Il ne peut y avoir quelqu'un d'autre prenant le contrôle sur les données d'un autre utilisateur. Une clé privée unique identifie l'utilisateur.
- Le système est "auto-géré", aucune entreprise ni gouvernement n'a la main dessus, donc aucune porte dérobée ni moyen de détourner les informations cryptées.

- Comparé à d'autres systèmes de centralisation, celui-ci permet la sécurité, la gestion des données par le client, et la mise en commun des informations pour les entreprises.

4. Analyse de risques, comparaison à l'offre existante et aux offres de substitution

Nous avons trouvé 2 méthodes existantes, fournissant un service pouvant se rapprocher du KYChaine :

a. Base de données interne

La première méthode est celle utilisée dans notre société aujourd'hui. Chaque service (Entreprises, Banques, CAF) possède leurs propres documents relatifs aux utilisateurs. Cette méthode comporte plusieurs inconvénients :

- Il y a des doublons de données entre les services, et plus généralement entre les entreprises. Chacun à sa copie de la donnée chez lui.
- Il est plus simple pour un hacker de trouver une faille dans un système d'une seule entreprise.

L'avantage de cette méthode est que chaque organisme possède ce que l'utilisateur veut lui fournir, et dans les consciences, les entreprises préfèrent avoir les données sauvegardées chez eux, et même avec encore de nos jours, une copie papier.

b. Base de données centralisée

Une autre idée qui revient est celle de la centralisation des données. Cette idée est plutôt avantageuse pour plusieurs points :

- Les démarches administratives sont plus simples : la donnée est à un seul endroit. L'accès est régulé ou non par l'utilisateur.
- Pas de doublons inutiles entre les services ou les entreprises, car toutes accèdent la même donnée.
- La réécriture en cas d'erreur est possible en remplaçant l'ancienne version de la donnée, et est immédiate pour tous les tiers utilisant ce service.

Cette méthode bien qu'avantageuse contient néanmoins d'importants problèmes liés à la sécurité :

- L'administrateur possède les infos de tout le monde et y a accès en clair. Il y a donc une faille car l'administrateur peut les utiliser à des fins non honorables.
- En cas de faille dans le système, il est possible de récupérer toutes les données de tout le monde en un seul coup pour un hacker.
- Suite à une erreur ou un hacking, toutes les données peuvent être perdues.
- Ce n'est pas l'utilisateur mais l'administrateur qui est le seul à choisir les données partagées pour chaque organisme.

Pour résumer, voici un tableau synthétisant les inconvénients puis les avantages de chaque méthode :

	Base de données interne	Base de données centralisée	KYChaine
Sécurisé contre le vol de données	KO	KO	OK
Personne n'a accès à toutes les données	KO	KO	OK
Réécriture possible des données	OK	OK	KO – OK
Pas de doublons inutiles	KO	OK	KO – OK
L'utilisateur est maître de ses données	OK	KO	OK
Démarches administratives plus simples	KO	OK	OK
Impossibilité de perdre des données	KO	KO	OK

5. Business Plan (dont étude de marché)

a. Le marché

Tout citoyen est "client" de ce marché. Toute entreprise ou organisme l'est aussi, en tant que client aussi, dans une autre mesure. Nous touchons donc le marché des données personnelles, privées et publiques des utilisateurs. La clientèle de ce marché est ainsi diversifiée. La société toute entière pourrait potentiellement utiliser ce service, dans tout ce qui est rapport entre les clients et les entreprises.

Le marché de la gestion des données personnelles est très récent. Cette question est nouvelle et apporte son lot de propositions diverses et variées sur le marché.

Le principe de KYC est utilisé dans beaucoup de secteurs (banques, assurances, notaires, courtiers, huissiers de justice, avocats, casino, bookmaker, etc.), soit à peu près tout ce qui implique des transactions monétaires.

Cette technologie permet d'éviter de nombreux vols d'identité ou autres fraudes. Des statistiques réalisées au Canada par le ministère de la sécurité publique du Québec ont indiqué une hausse des vols d'identité de près de 20 % ces 2 dernières années. Pour 58 % des victimes, la perte financière serait inférieure à 100 $, mais 6 % ont eu des pertes supérieures à 5 000 $. Ces pertes sont parfois imputées à l'utilisateur mais parfois aux banques, ou autres tierces entreprises sur lesquelles la transaction a été effectuée. Ainsi, ces fraudes engendrent des pertes pour tous, et donc notre solution peut être profitable à tout le monde.

b. La concurrence

Après diverses recherches, nous constatons qu'il y a peu de concurrents directs, proposant une plateforme permettant de partager ses données privées. Les seuls services entrepris à notre connaissance sont faits par le gouvernement français et une autre entreprise. Le but du gouvernement

est de collecter les données privées des utilisateurs et de les mettre dans une base de données. Ce n'est donc pas un concurrent car le résultat attendu n'est pas le même. En effet, leur but est de se servir personnellement de cette base de données, et non pas de mettre en relation les entreprises et les utilisateurs.

L'autre service est appelé "Storj". C'est une plateforme de Cloud, qui s'appuie sur la technologie du Blockchain. Comme notre projet, elle se sert de cette technologie pour transférer des données personnelles. Mais contrairement à notre solution, elle est utilisée seulement pour un usage personnel de l'utilisateur. Ainsi, ce concurrent ne joue pas sur le même marché que nous.

c. La réglementation

Les données personnelles sont, dans l'Union Européenne, encadrées par des lois afin de les protéger au mieux. Leur utilisation abusive, comme par exemple une utilisation à but commercial, est prohibée en Europe. Il n'y a aucune répercussion directe sur notre projet, étant donné que nous ne stockons pas, ni n'avons accès à ces données personnelles. Elles n'existent publiquement que d'une manière cryptées et déchiffrables uniquement par le propriétaire de ces données. Il nous faut seulement garder à l'esprit que nous gérons des données privées et personnelles, et qu'il faut ainsi que notre solution soit sans faille au niveau de la sécurité.

d. Coût actuel du processus de KYC

Il est assez difficile de fournir une idée du coût du processus étant donné qu'il est loin d'être standardisé. Il est par contre certain que ce coût augmente lorsque le nombre de client et de contrat important augmente. Car dans ce cas, des recherches plus profondes et méticuleuses sont faites, cela prend plus de temps et de ressources donc d'argent. Un autre point certain est le fait que le coût du KYC est élevé. Mais si le KYC n'est pas fait, le coût est encore plus important à cause des pertes en fraude, de l'usurpation d'identité...

Selon une étude de Thomson Reuters en 2016 sur 800 institutions financières, 89% ont une mauvaise expérience interne avec le processus de KYC. La moyenne des dépenses de ces institutions est de 60 millions de $ par an (et 500 millions pour les plus grosses). 60% de ces institutions ont déclaré avoir amélioré leur processus au cours de la dernière année (impliquant des dépenses plus importantes).

La donnée la plus importante est que 30% des institutions disent que leurs clients ne sont pas proactifs dans la communication des changements les concernant, provoquant une surcharge de travail de la part des entreprises pour récupérer les nouvelles informations (typiquement, une carte d'identité périmée).

Aussi, le coût varie d'une entreprise à une autre selon beaucoup de critères :

- Les enjeux business et la taille du portefeuille client : secteurs couverts, solvabilité, historique de la relation, etc.
- Les coûts structurels inhérents à l'activité : les ressources matérielles et humaines nécessaires.
- Les processus internes et de l'organisation de l'activité : tâches manuelles ou automatisation.
- La prise en compte des risques réglementaires (FATCA, Lutte anti-blanchiment, etc.)
- etc.

Il y a donc beaucoup de paramètres matériels, logistiques et humains qui permettent de chiffrer le coût de ce principe de vérification d'identité client. Il faut aussi garder en tête que dans beaucoup d'entreprises, la communication entre les services n'est pas toujours parfaite. Souvent, les services ne partagent pas la même base de données, augmentant donc la complexité et les coûts de traitement.

La situation actuelle étant ainsi représentée, notre solution s'installe parfaitement dans cet environnement requérant une solution efficace.

e. Coût de notre solution : KYChaine

Notre solution a un certain coût, pour l'organisme lançant cette initiative (en l'occurrence nous, KYChaine) mais aussi pour les entreprises adhérentes. En outre, cette solution est gratuite pour les clients finaux.

i. Pour l'organisme

Pour l'organisme, c'est un coût de lancement d'activité, de démarchage, de commercialisation, de publicité, etc.

Il faut ajouter à cela le coût d'un serveur afin de s'interfacer avec la blockchain et y rentrer des informations, ainsi que le coût de maintenance de ce serveur. Car plus il y a d'utilisateur utilisant notre service, plus le risque d'un problème est important, et il faut donc y pallier rapidement.

ii. Pour les entreprises

Pour les entreprises adoptant cette solution, il y a un coût d'infrastructure pour stocker la blockchain et la faire vivre. Mais il y a surtout un coût pour transférer toutes les données en cette plateforme, ou pour utiliser en parallèle l'ancienne et la nouvelle solution le temps de tout migrer. Sur le long terme, ce coût est négligeable et il ne reste plus que le coût de l'activité manuelle et les ressources engendrées, en prenant en compte que cette solution favorise l'automatisation et réduit énormément les démarches, et donc réduit les coûts inhérents.

Pour fonctionner, la blockchain nécessite une puissance de calcul importante pour assurer l'authenticité des transactions. Ces nœuds de calcul seraient donc répartis entre les différents organismes souhaitant bénéficier du service. Cela correspondrait donc à un coût d'utilisation, car pour utiliser le service, on doit lui permettre de vivre. On pourrait au sein de ces organismes retrouver des banques, des gouvernements, de grandes organisations immobilières, etc. Pour disposer d'un système accessible à tous, certains petits utilisateurs tel qu'un bailleur indépendant souhaitant s'assurer de la solvabilité de son futur locataire pourrait soit contribuer au réseau en validant des transactions, soit payer un certain montant pour utiliser le service. Ainsi, tous les acteurs financent la solution et la font vivre selon leurs moyens respectifs.

f. La rentabilité

En investiguant sur les coûts actuels de KYC d'après les différents sondages et études, on comprend bien que ce processus est coûteux aux entreprises. Un petit ajustement bénéfique sur le traitement de ces données peut avoir un impact immense réduisant les dépenses liées au KYC. Ce processus est encore très souvent manuel, et bien que parfois automatique, il reste fastidieux. Notre solution permet facilité, automatisation, ce qui impliquera sur le long terme une rentabilité pour l'entreprise concernée. Aussi, avec un mécanisme simplifié et plus efficace, celle-ci pourra se focaliser sur le traitement de l'information. D'après le Fonds monétaire international, le volume du blanchiment

d'argent dans le monde se situe entre 2 et 5 % du PIB mondial. Ce blanchissement d'argent n'est surement pas dû uniquement au manque de connaissance du client, mais une bonne partie peut être évitée en améliorant ce principe. Le processus de KYC est donc un processus rentable bien que coûteux. Le challenge est donc de rendre ce processus moins coûteux, et c'est dans cette optique là que nous nous plaçons. De plus, le blanchiment d'argent n'est pas la seule fraude impliquant des pertes pour les entreprises. Nous ne pouvons pas chiffrer ces pertes futures, mais nous pouvons aisément placer une hypothèse simple : celle que KYChaine facilitera la collecte des données. Les entreprises se concentreront donc sur le traitement des données et pourront ainsi réduire leurs pertes dues aux fraudes.

6. Spécifications techniques et pistes de développement

Le chapitre suivant va détailler les différents choix que nous avons réalisé sur un plan technique. Nous allons aborder la blockchain, qui est le cœur du projet, certaines notions de cryptographie et finalement les choix de notre architecture et les connexions avec l'interface utilisateur.

a. Blockchain

Disposer d'un stockage public, sûr et décentralisé était la problématique même de notre projet. La blockchain répond parfaitement à ces besoins, nous avons donc dû choisir entre réimplémenter une solution répondant parfaitement à nos besoins en prenant le risque de laisser des failles de sécurités ou des erreurs. Notre choix c'est plutôt porté sur une implémentation existante au vu du faible temps disponible pour réaliser le POC. Nous avons choisi Multichain, une implémentation open-source ayant pour base la blockchain du Bitcoin. Cette implémentation remplit notre cahier des charges en fournissant la possibilité de stocker des informations brutes et en proposant une gestion des droits d'accès avancée.

Multichain nous permet de construire simplement un réseau peer to peer mettant en relations les mineurs qui vont valider les transactions du réseau. Il propose des API avec différents langages dont Javascript sur lequel nous avons basé notre POC.

Les informations utilisateurs sont stockées au format XML. Ce format de données est plutôt verbeux mais il a le gros avantage de proposer un système de vérification d'intégrité. Nous pouvons ainsi nous assurer que tous les messages postés sur le réseau soient cohérents et complets.

Multichain utilise des entrepôts de données pour stocker des informations brutes. Ils sont appelés « stream » et vont contenir les informations utilisateurs tel que les données ou les mots de passes. On peut les représenter sous la forme d'un dictionnaire, chaque valeur publiée à l'intérieur est identifiée par une clef.

Les clés utilisées pour le stockage des informations ont la forme suivante :

<adresse_utilisateur>/<clef_de_la_donnée>

b. Cryptographie

Il existe de nombreuses explications sur internet à propos de la cryptographie, nous nous contenterons simplement d'aborder les termes généraux.

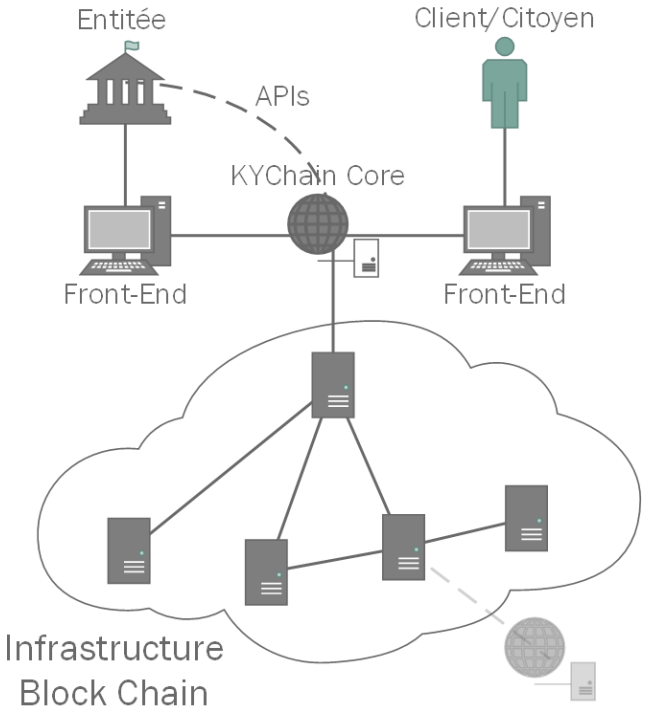
Nous utilisons, comme indiqué précédemment, deux mécanismes de cryptographie : l'un symétrique et l'autre asymétrique.

La partie symétrique est assurée par l'algorithme AES, le mot de passe que nous utilisons pour encrypter les données utilisateurs est une chaîne alphanumérique de 64 caractères.

La partie asymétrique repose quant à elle sur l'algorithme RSA. La sécurité dans RSA repose sur un couple de nombre premiers, la force du protocole dépend de la taille de ces nombres. Une taille de 4096 bits est un standard nous assurant quelques années de tranquillité en termes de sécurité.

c. Architecture et interface utilisateur

L'architecture de la solution repose principalement sur la blockchain qui sécurise les données et leurs accès. Afin de faciliter l'utilisation de la solution, nous avons déployé une interface web permettant à un client de consulter et de partager simplement ses informations sur la blockchain.



Les utilisateurs et les entités se connectent via l'interface web, qui va contrôler et simplifier les démarches. Cette interface communique ensuite avec le réseau de la blockchain pour accéder aux informations.

Dans cette configuration initiale, il n'existe qu'une interface web unique pour tous les acteurs. À terme, chaque entité pourra avoir une interface personnalisée interagissant avec son système d'information.

d. Webographie

- Trulioo, [consultation : mars 2017]. Le processus est les pratiques du KYC. Disponible sur : https://www.trulioo.com/blog/know-your-customer-kyc-due-diligence-best-practices/
- Trulioo, [consultation : mars 2017]. Les coûts du KYC. Disponible sur : https://www.trulioo.com/blog/kyc-costs-rising/
- KYCMap, [consultation : avril 2017]. Législation française du KYC. Disponible sur : http://kycmap.com/france-know-your-customer-kyc-rules/

- Ministère de la sécurité publique du Québec, [consultation : février 2017]. Statistiques de fraude au Canada. Disponible sur : http://www.securitepublique.gouv.qc.ca/police/publications-et-statistiques/autres-statistiques-criminelles/sondage-vol-identite/les-victimes-de-vols-d-identite.html
- PwC France, [consultation : mai 2017]. Législation française du KYC. Disponible sur : https://www.pwc.com/gx/en/financial-services/assets/pwc-kyc-anti-money-laundering-guide-2013.pdf
- Gouvernement français, [consultation : mai 2017]. Lutte anti blanchiment et terrorisme. Disponible sur : http://www.economie.gouv.fr/tracfin/accueil-tracfin
- Thomson Reuters, [consultation : février 2017]. Sondage sur les entreprises vis à vis du KYC. Disponible sur : https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html
- Multichain, [consultation : janvier 2017]. Solution de blockchain open-source. Disponible sur : http://www.multichain.com/