Publié dans MesInfos le 07/02/2017 (dernière mise à jour le 07/02/2017)
Tags : A la UneUncategorized
http://reseau.fing.org/blog/view/168788/les-rencontres-du-self-data-%C2%AB%C2%A0les-architectures-et-defis-techniques-du-self-data%C2%A0%C2%BB
Page générée le 23/08/2017 à 23:41

Les rencontres du Self Data : « Les architectures et défis techniques du Self Data »

Nous avons tenu la seconde de nos Rencontres Du Self Data le 13 décembre 2016. Elle s'inscrit dans le cadre du pilote MesInfos – qui rassemble l'effort collectif de différentes entreprises de s'engager concrètement dans le Self Data. Ces entreprises restituent ainsi en 2016 et 2017 pour la première fois de manière pérenne les données de leurs clients à leurs clients, pour qu'ils en fassent ce qui a du sens pour eux.

L'objectif de cette seconde rencontre était d'explorer plus profondément les défis techniques du Self Data : comment les organisations restituent-elles les données ? Via quels canaux de transmission ? Sur quels espaces de stockage et d'administration personnel pour les individus ? Pour quelle sécurité ?

Sans réponses à ces questions, le Self Data, ne deviendra jamais réalité. Quatre intervenants ont pu présenter leurs pistes de réflexions et d'action, leurs questionnements, leurs impressions et échanger avec les participants sur ce défi technique essentiel à la création d'un monde de Self Data :

- Serge Abiteboul chercheur à l'Inria replace le contexte actuel « data-esque » dans lequel nous évoluons en tant qu'individu et dessine un horizon de solutions de systèmes d'informations personnels : les Pims (Personal Information Management System) ;

- Guillaume Jacquart coordinateur technique du Pilote MesInfos nous raconte comment le pilote offre lui-même quelque pistes de réponses, car il met en pratique le Self Data : méthode employée pour restituer les données, difficultés rencontrées, pistes pour l'avenir… ;

- Paul Tran-Van, doctorant chez Cozycloud (Pims) et à l'Inria, partage ses travaux sur les moyens techniques et les problématiques de restitution des données aux individus ainsi que sur les supports de récupération, de stockage et d'administration des données par les individus ;

- Jorick Lartigau, responsable R&D de MatchupBox, solution de partage et de stockage de ses données nous parle de « Privacy by design » et de leur architecture orientée « P2P/Blockchain.

Cet article est une adaptation écrite de leurs interventions.

1 – Serge Abiteboul : Les Personal Information Management Systems (Pims), outils techniques du Self Data ?

Serge Abiteboul commence par nous interpeller : essayez de comptabiliser le nombre de données que vous générez chaque jour ; recensez les organisations avec lesquelles vous êtes en relation en ligne et hors ligne. Le nombre de données donne le vertige mais c'est surtout la fragmentation de celles-ci sur tant de système différent qui frappe. Vous n'avez ni vue globale ni contrôle, vous êtes le prisonnier de ce système, vous perdez votre vie privée et votre liberté.

Un constat plutôt inquiétant, qu'il contrebalance en nous proposant trois alternatives :
- Ne faites rien, c'est trop tard et ça va devenir de pire en pire
- Collectez vos données, changez de fournisseurs de service, organisez votre gestion de données, passez-y des heures (seulement pour ceux qui en ont la capacité techniques, les "geeks").
- Donc si vous n'êtes pas geeks, mettez-vous au boulot pour le devenir rapidement.

Vous l'aurez compris, ce ne sont pas vraiment des alternatives très alléchantes… Une solution pourtant semble se distinguer, au nom encore un peu complexe : les Pims (Personal Information Management System) – un système d'information personnel qui permet d'agréger toute ses données, de les stocker de manière sécurisée et de les administrer, d'en tirer une valeur d'usage grâce à des services tiers, des applications, qui tournent dans le Pims.

Certains parlent d'un système "dans les nuages", accessible partout et à tout moment, d'autres estiment qu'il faut centraliser ce système personnel… Mais l'idée est bien celle d'un même système personnel pour toutes ses données. Une idée aussi vieille que l'informatique nous révèle Serge Abiteboul. Tous les 10 ans, un nouveau gourou nous l'annonce, sous un nom différent mais couvrant le même genre d'idée.

Si on me l'annonce tous les 10 ans, alors pourquoi devrait-on prendre l'annonce des "Pims" au sérieux ?

D'abord parce que le volume d'information augmente, la façon dont on travaille aujourd'hui fait que les données des services web, sont sur des machines on ne sait où, dans on ne sait quel pays, sous on ne sait quelle législation, avec quel logiciel… L'idée du Pims est donc de pouvoir avoir mes données sur ma machine, avec un logiciel dont je sais ce qu'il fait, en lequel je peux avoir confiance.

La difficulté est que ces services web éparpillés sont particulièrement utilisés et qu'il est difficile de les quitter pour tout faire depuis son propre serveur. Je peux donc en tant qu'individu accepter que le service que j'utilise dispose de mes données, mais le minimum c'est que moi aussi je puisse en disposer, en avoir une copie.

Les 3 raisons pour lesquelles l'avènement des Pims est proche

1) les raisons sociétales

- Les gens en ont assez de la façon dont leurs données sont exploitées, de l'asymétrie entre eux et les organisations
- Les gouvernements européens passent des lois et des règlements qui vont dans le sens des Pims : protection, portabilité, transparence…
- Des initiatives pour que les organisations partagent avec les individus les données qu'elles ont sur eux existent : le projet Mesinfos porté par la Fing et d'autres (MiData, Les "Buttons" américains, …)

2) les raisons technologiques

- Le prix des machines est tombé. Il y a 10 ans si l'on voulait s'acheter une machine, l'installer « chez soi » coûtait très cher. Aujourd'hui une machine virtuelle hébergée par OVH coûte quelques euros par mois.

- De nombreuses personnes développent des technologies (par exemple CozyCloud) et n'importe qui aujourd'hui peut décider d'avoir son propre serveur pour ses mails.

3) les raisons industrielles

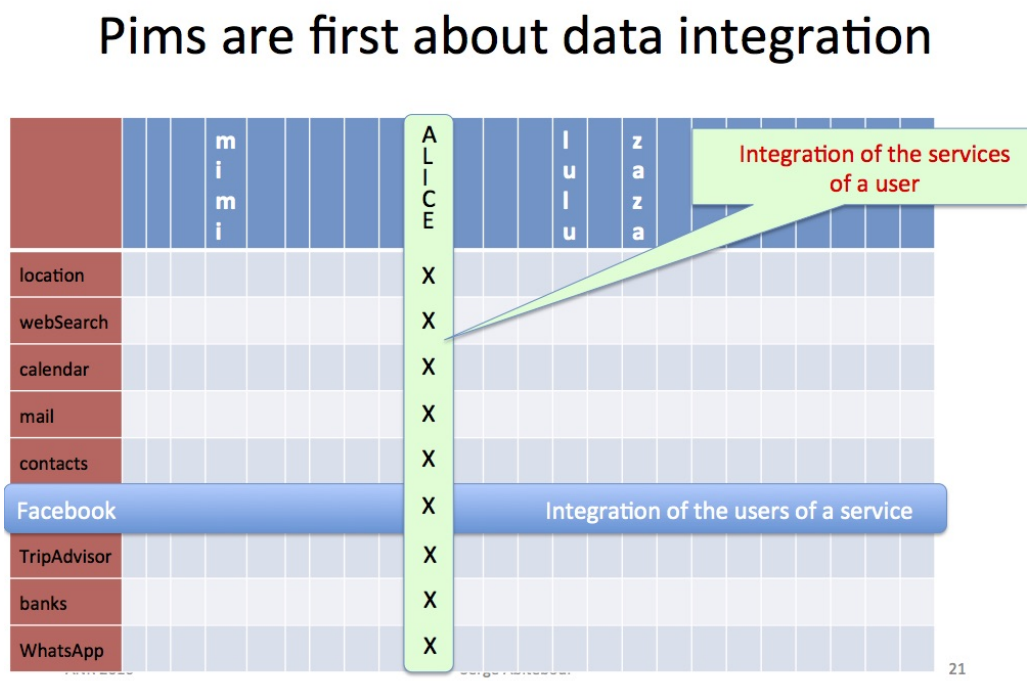
- Les entreprises préindustrielles (banque, assurance…) savent gérer leurs clients mais ne sont pas les plus douées numériquement. A titre d'exemple, la plateforme Booking s'est placée entre les hôteliers et leurs clients et "mangent" leur marge. Avec les Pims, elles peuvent aller sur un terrain plus familier.

- Certaines entreprises disposent déjà d'un capital "confiance" : les individus installent chez eux la boxe de leurs fournisseur internet, c'est comme si ils acceptaient d'installer leur ordinateur chez eux. Pourtant, ces entreprises ne sont pas assez proactives sur la question du serveur personnel, selon Serge Abiteboul, c'est un peu décevant car elles seraient en pôle position pour proposer des Pims.

- Les "Pure Internet Players" adorent les données personnelles – leur ADN repose sur elles, particulièrement leur business model, car ils les commercialisent. Ils seraient les meilleurs pour proposer des Pims, mais le passage de la commercialisation à la protection des données personnelles n'est pas dans leur état d'esprit.

Les avantages des Pims sont nombreux…

Si les individus ont leurs données dans un même système, ils pourront faire des choses nouvelles. C'est vraiment la différence entre une vision "service web" éparpillés et une vision "Pims".



- A l'horizontale, sont présents tous les services web utilisés ou utilisables par un individu, ses données sont éparpillées.
- A la verticale, la vision Pims – l'individu peut faire du croisement de données, la valeur d'usage est beaucoup plus forte.

… mais les difficultés sont également fortes !

- "Je veux bien que le monde soit meilleur mais je ne veux pas changer de téléphone, J'aime beaucoup mon éditeur de texte, je veux bien un nouvel éditeur qui protège mes données mais je veux exactement le même". Les gens n'adhèrent pas à de nouveaux services comme les Pims sur le seul argument moral.

- Comment faire de la 0 administration ? Si les individus décident d'avoir un Pims, ils ne souhaitent pas l'administrer quotidiennement, cela ne doit pas demander trop de travail.
- La sécurité : à partir du moment où j'agrège toutes mes données dans un même espace, il faut qu'il soit extrêmement sécurisé. Car si quelqu'un rentre dans votre Pims, il aura toutes vos données. Même si le stockage des différents Pims est décentralisé, la sécurité pour chacun d'entre eux est une priorité.

Rebondissant sur la présentation de Serge Abiteboul, les participants soulèvent la question du volume des données : l'espace de stockage de mon Pims ne devra-t-il pas s'élever à des chiffres très élevés ? Et surtout, à quoi servent réellement les Pims ? Quelle est la valeur d'usage pour l'individu ? Il existe déjà des choses assez bluffantes sur le croisement des données avec les services d'assistants personnels, les services prédictifs. S'ils "tournaient" au sein du Pims de l'individu, ils seraient bien moins risqués pour la vie privée de ce dernier. Le projet MesInfos travaille à déterminer les usages possibles du Self Data et en recense de nombreux cas.

La vision globale dont l'individu dispose grâce à son Pims est une force, c'est aussi un espace qui permet à chacun de se "libérer" des services web actuel, la plupart des individus se servant de ces derniers pour stocker et administrer certaines données (par exemple Facebook pour les photos). Quelle est la valeur pour le système ? Cette valeur sera-t-elle suffisamment forte pour tirer les Pims vers le haut de l'affiche ? Le fait qu'un Pims puisse croiser les données permet d'imaginer de nouveaux usages supposés transformer nos vies. Par exemple les secteurs des transports, de médecine, demandent ce genre de croisement de données diverses et multiples.

Retrouver la présentation de Serge Abiteboul ici.

2 – Guillaume Jacquart, coordinateur technique du projet MesInfos : quels sont les grands enjeux techniques du Self Data ?

En 2016 la Fing a lancé un pilote ambitieux, des partenaires (entreprises, collectivités) s'engagent à restituer les données personnelles qu'elles détiennent sur 3000 de leurs clients et usagers.

Il ne s'agit pas d'une expérimentation mais bien d'une restitution de manière pérenne, les entreprises ont dû recenser les données,

développer les canaux de transmission des données (API), et s'assurer que les individus puissent les récupérer et les utiliser de manière sécurisée sur leur espace personnel, leurs "Pims" (Cozy Cloud pour les 3000 testeurs, avec comme objectif d'ouvrir à d'autres plateformes).

Mais quelles sont les différences d'hébergement entre "Pims" ?

- Cozy Cloud : l'hébergement de son serveur personnel peut se faire chez OVH en France ou sur une machine, chez soi.
- Digime : l'hébergement peut se faire sur son téléphone portable ou sur des services en lignes de stockage (comme DropBox). Dans ce dernier cas les données sont cryptées.
- Matchupbox : L'hébergement se fait de manière distribuée, en P2P. Jorick Lartigau le présente plus bas.
- Autres solutions : l'hébergement se fait sur un serveur centralisé (chez un fournisseur d'hébergement), et repose sur la confiance que les individus ont dans la sécurité du serveur.

Quelques leviers de développement du Self Data :

- Une augmentation du volume et de la diversité des données – des services peuvent faire des premiers croisements de données et ouvrir de nouveaux univers d'usage.

- Le GDPR instaure le droit à la portabilité, les entreprises doivent se mettre en conformité pour 2018 et permettre aux clients qui le leur demandent d'"emporter" leurs données ailleurs (dans leur "chez eux numérique", chez une autre organisation, chez un service tiers, …).

Dans le cadre de ce droit à la portabilité, les organisations cherchent des solutions pour mieux se rendre compte d'où se trouvent les données personnelles dans leur système d'information, comment identifier dans leur système les individus qui demandent à exercer leur droit à la portabilité afin d'être sûr de restituer les données aux bonnes personnes… C'est le travail que la Fing et ses partenaires réalisent dans le cadre du Pilote MesInfos. Les testeurs du pilotent "emportent" leurs données depuis l'organisation avec laquelle ils sont en relation jusqu'à leur Cloud Personnel, leur "chez eux numérique", bref leur Cozy, pour en tirer une valeur d'usage. C'est un moyen de concilier deux élans : reconstruire la relation client et répondre à la mise en conformité avec la nouvelle régulation européenne.

Un autre règlement européen fait levier : l'"eIDAS" qui oblige chaque Etat à disposer d'un moyen standard pour permettre à chaque citoyen de s'identifier/s'authentifier facilement face à une organisation, un service public. En France le dispositif est France Connect. Ces genres de dispositifs sont des socles importants pour le Self Data : on pourrait imaginer se connecter avec un seul et même identifiant à toutes les organisations avec lesquelles on est en relation pour récupérer ses données.

Un débat sur l'intérêt de la BlockChain dans ce cas précis de l'identification est ensuite soulevé par les participants. C'est en effet possible d'imaginer cela nous raconte Guillaume Jacquart, après tout Ethernum cherche à fédérer les identités stockées dans la BlockChain, mais elle sert alors plus de base de données distribuée que d'outil d'identification/d'authentification. La question principale de lier identité réelle et identité numérique n'est pas réglée magiquement par l'utilisation de la BlockChain, nous avons besoin d'outils comme France Connect. Et Jorick Lartigau de continuer sur cette lancée : "la blockchain n'est pas figée, elle peut-être vue comme une base de données distribuée, l'usage que vous en faite vous appartient".

Quelle interopérabilité entre Pims ?

Aujourd'hui beaucoup d'acteurs se connaissent, se parlent de manière amicale, affichent qu'ils font des choses ensemble, mais beaucoup se voient comme concurrents. Or la logique de "il n'en restera qu'un à la fin" n'a pas vraiment de sens dans un monde de Self Data capacitant pour les individus : le vrai pouvoir des individus est de leur laisser la possibilité de changer de plateforme de gestion de leurs données personnelles.

Serge Abiteboul renchérit : l'attractivité d'un service comme Booking est justement d'avoir tout le marché, or les Pims n'ont pas besoin de cela pour être attractifs.

C'est le sens que Guillaume Jacquart donne à cette coopération entre Pims : la grande partie de la valeur viendra des usages proposés, or aucun Pims n'est capable de produire seul tous les cas d'usages possibles et imaginables. L'ouverture entre Pims est donc nécessaire pour favoriser une dynamique de réseau : les individus doivent en effet pouvoir tirer parti de leurs données grâce à des services tiers, installés si possible sur leur Pims. Un service qui se développe sur Cozy devrait donc être compatible avec Pickio, Digime ou toute autre plateforme.

Peut-on imaginer des "standards de services" pour des plateformes aux architectures assez diverses ? Quelques pistes existent déjà :
- Remote storage : cela peut constituer une brique de base – on pourrait avoir des services web qui demandent à l'individu où il souhaite stocker ses données.

- Des standards utiles entre les détenteurs de données et les plateformes – par exemple le protocole OSE2. Certaines difficultés apparaissent par contre avec les différences d'architecture des Pims.
- Un protocole dédié à cet univers : UMA (User Manage Access), un système qui va permettre le contrôle par une machine de l'autorisation de l'individu sur l'accès des services tiers à ses différentes données. Par exemple si vous donnez quelques règles à votre Cozy, et que vous "branchez" votre Cozy à votre Frigo, il va pouvoir converser avec les API de distributeur, sous votre contrôle.

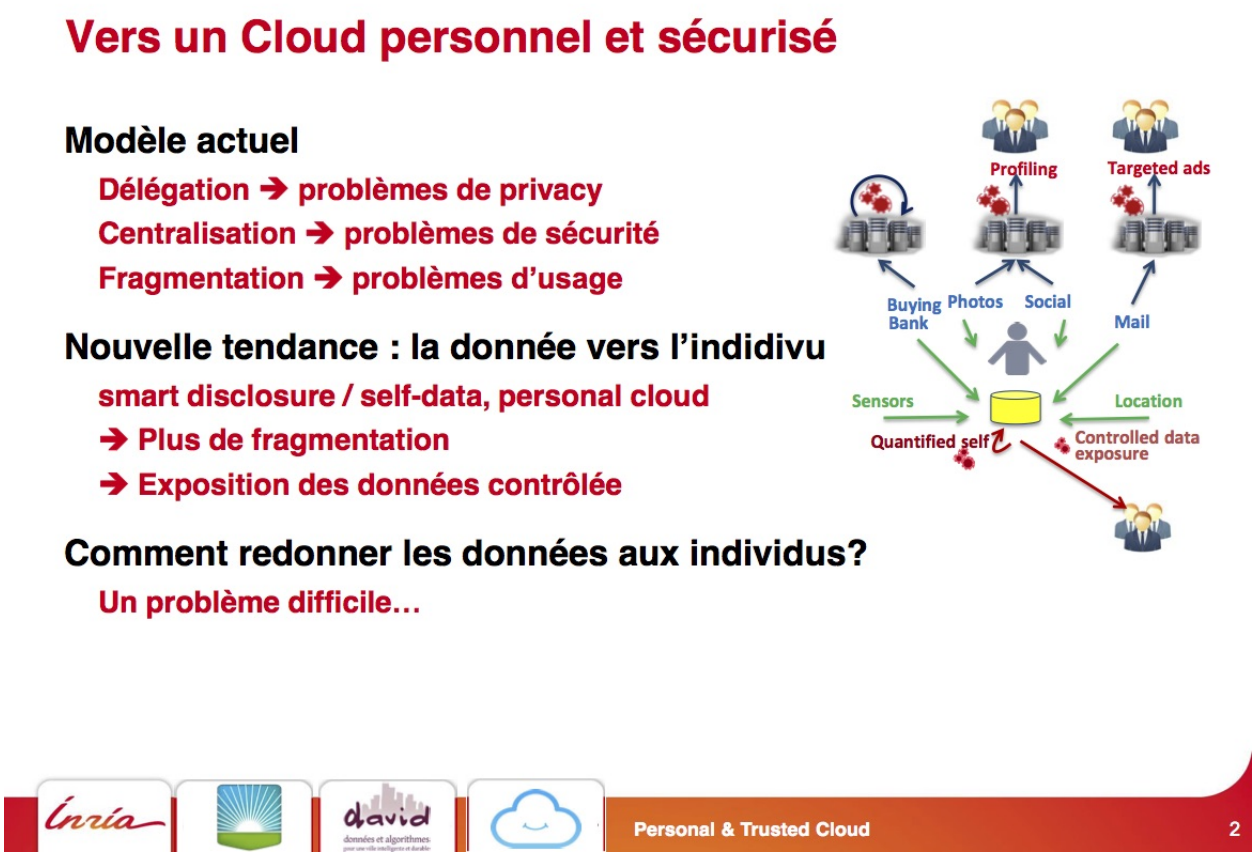
Et la planète ?

La question environnementale lorsqu'on parle données relève aujourd'hui d'une volonté personnelle ou politique, sera peut-être une nécessité dans 10 ans. Si le Self Data permet à l'individu de mieux se connaître, d'agir selon ses valeurs et de consommer de manière plus éthique ou plus écologique, comment comparer ces bénéfices par rapport à l'empreinte écologique des outils du Self Data (Pims, Applications, API, stockage des données …) ?

Retrouver la description du pilote MesInfos ici : http://mesinfos.fing.org/participer/

3 – Paul Tran-Van, doctorant, CozyCloud et Inria : agréger, sécuriser et partager des données personnelles, 3 défis du Self Data.

Le modèle actuel d'internet pose de gros problèmes de sécurité et d'usage, les données étant dispersées. Mais une nouvelle tendance (que certains appellent Pims, VRM, Self Data) va vers l'inversement de cette chaîne de valeur : l'individu sera au centre de ses données.



Les plateformes de Cloud Personnels, les Pims comme Guillaume Jacquart et Serge Abiteboul les ont appelés précédemment – par exemple Cozy – sont des outils pour permettre aux individus d'être au centre de leurs données.

Premier défi : agréger les données

L'application Konnectors dans Cozy permet aux individus de rapatrier leurs données dans leurs Cozy. Ils sélectionnent l'organisation avec laquelle ils sont en relation (SFR, Améli, DirectEnergie, …), renseignent leur mot de passe et leur identifiant et le "konnector" va fonctionner comme un logiciel de scraping pour collecter l'ensemble des données et documents de leurs espaces clients et les stocker dans leurs Cozy.

Deux problèmes avec cette pratique :
- Si l'organisation effectue une refonte de son site/espace client, il faut entièrement recréer le "konnector".
- Ces "konnectors" ne sont pas particulièrement appréciés par les organisations, et parfois sont interdit dans les CGU que les utilisateurs signent.

Avec l'application du droit à la portabilité du GDPR en mai 2018, on peut espérer un développement d'API par les organisations qui permettrait de résoudre cela.

Certaines entreprises se spécialisent par exemple dans le développement de connecteurs bancaires. L'intérêt des plateformes de Cloud Personnel comme Cozy, c'est que cela permet le croisement de données qui apporteront une valeur d'usage à l'individu (par exemple croiser données bancaires et données de consommation énergétique).

Ce premier défi résumé par Paul Tran Van interroge : comment un service va pouvoir utiliser des données d'origines différentes? Quels sont les formats des données que je peux récupérer ? Dans beaucoup de cas les konnectors de Cozy donnent du PDF, les données ne sont alors pas machine-readable mais human-readable. D'où l'intérêt de voir se développer des API par les organisations.

Second défi : sécuriser les données

Autre grand défi : la sécurité. Un sondage des utilisateurs de Cozy cette année permet de se rendre compte que pour eux la priorité la plus importante pour un Cloud Personnel étaient l'éthique (le Cloud ne doit pas m'espionner) et la sécurité, loin devant l'expérience utilisateur !

Ce qui est également difficile c'est que si les utilisateurs souhaitent la sécurité ils ne sont pas prêts à faire des concessions sur la facilité d'usage.

Une autre expérimentation menée permet de se représenter cette priorité de sécurité chez les utilisateurs.
- un groupe doit répondre à des questions personnelles, on leur précise que leurs réponses seront stockées sur un serveur centralisé
- un groupe doit répondre à des questions personnelles, on leur précise que leurs réponses seront stockées sur une clé USB à laquelle personne n'aura accès.

Il y a t-il une différence dans les réponses aux questions ? Aucune ! Ils sont sensibles à la vie privée mais répondent aux mêmes questions quelque soit la façon dont leurs données sont stockées. Cela démontre la difficulté qu'il y a à faire comprendre la sécurité d'un système à des utilisateurs.

Troisième défi : partager les données

Agréger ses données dans un espace sécurisé c'est bien mais les utilisateurs ont envie de les partager, pas de les enfermer. L'une des questions récurrente des utilisateurs de Cozy est donc "quand est-ce que je vais pouvoir partager certaines données de mon Cozy avec des amis, de la famille, des organisations ?"

Le Laboratoire SMIS (Inria) a développé une solution de stockage sécurisée : PlugDB, une clef USB sur laquelle les données sont chiffrées avec un moteur de données embarqué pour requêter les données chiffrées et faire du traitement dessus sans jamais qu'elles sortent de la clef. C'est une garantie de sécurité très forte et on peut faire du traitement des données car le code est léger. En ce moment Cozy et le laboratoire SMIS travaillent ensemble. L'objectif est de brancher cette clef sur les serveurs Cozy et cela va être en charge du contrôle d'accès (« qui a accès à quelle donnée ») et du chiffrement.

Le sujet de l'interopérabilité est important pour le partage : un utilisateur de Pims veux pouvoir partager avec n'importe qui, même ce dernier n'est pas sur ce Pims. La priorité est donc de pouvoir partager au sein d'un même Pims (De Cozy à Cozy par exemple) mais également entre Pims de différents fournisseurs (de Cozy à OwnCloud par exemple).

Comment avancer sur ces questions ? Cozy a travaillé avec un community group du W3C, a écrit un dossier pour l'IETF et a conçu un POC pour créer les outils de partage entre Cozy et OwnCloud.

Sur cette dernière question du partage, la discussion avec les participants s'est tournée sur deux questions :
- La question du web sémantique, qui permettrait un partage efficace, mais qui demandent de créer des ontologies, de nouveaux protocoles. La première pierre à apporter est donc le partage via l'interopérabilité.
- La question de l'authentification et de la certification des données. Si je partage avec un tiers mes données, comment peut-il s'assurer que je l'ai modifié ou non ?

Retrouver la présentation de Paul Tran Van ici.

4 – Jorick Lartigau, responsable R&D de MatchupBox : privacy by design et architecture orientée P2P/Blockchain

MatchUpBox est une start-up qui est partie d'une idée folle il y a deux ans de faire un Facebook décentralisé, sans serveur. Beaucoup de choses existent déjà, si l'on remonte l'histoire de l'internet on trouve le P2P, le TCP/IP…

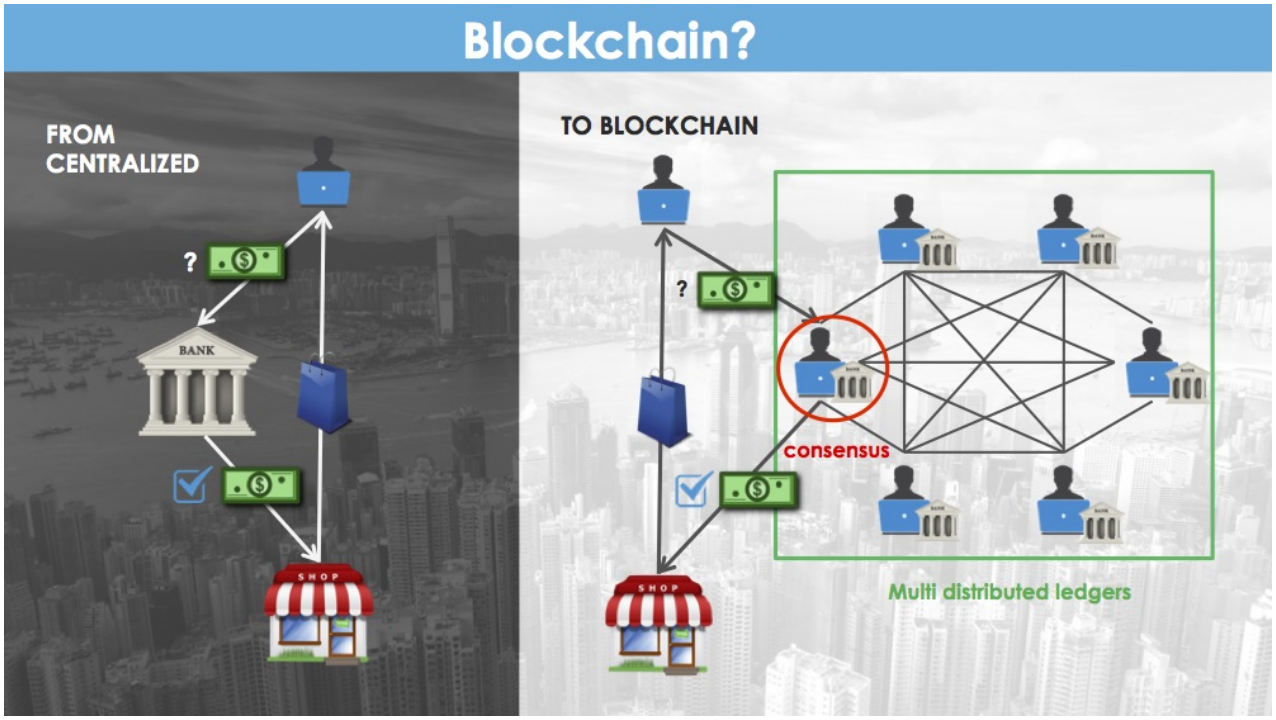
MatchUpBox et le stockage P2P

Pour une jeune start-up, réduire le coup de serveur à presque 0 est un avantage non négligeable. Un objectif : indexer les data, permettre aux utilisateurs de les utiliser, sans serveur.

Aujourd'hui si un utilisateur cherche un ami sur Facebook, il le cherche dans une grosse base de données, un énorme annuaire. Sans serveur (avec la technologie DHT utilisée par la BlockChain) chaque utilisateur peut héberger une partie de cet annuaire. Si l'utilisateur cherche Arthur, il va voir un noeud qui le renvoi vers Arthur. Tor permet d'anonymiser ces liens d'échanges. Si un tiers regarde le réseau et les utilisateurs qui communiquent en P2P, il va voir les adresses IP qui communiquent. Mais si il y a des intermédiaires entre eux, il ne peut voir que le noeud, et ni le receveur, ni l'envoyeur.

Comment ça marche ? Matryochka et BlockChain

Un individu A qui veut communiquer avec un autre individu B ne va pas le faire directement mais va le faire avec le point le plus éloigné qui dépend que du cercle de B. Une clef privée, sur la machine de A, permet également de signer les envois afin que B puisse certifier que le message vient bien de A.



Plusieurs problèmes sont identifiés dans la BlockChain. En dehors du réseau, rien ne rattache l'identifiant de A à son identité réelle (c'est pour cela que l'on dit que le Bitcoin est formidable pour le blanchiment d'argent).

La matryochka est un système de lettre digitale. La Blockchain permet elle de créer un système de lettre digitale recommandée.

Jorick Lartigau prend un exemple dans la santé : une entreprise qui permet à des patients à risques – équipés d'objets connectés – de recevoir des alertes ou d'en envoyer à des services d'urgence doit pouvoir faire remonter aux services d'urgences des données fiables (par exemple : Mr A est en train de faire un infarctus, il est de groupe AB+), d'où l'intérêt d'un échange "recommandé". Cela n'évite pas l'erreur si Mr A a mal renseigné son groupe sanguin, mais cela permet à l'entreprise qui alerte de prouver qu'elle a bien reçu cette donnée de cette personne.

Pour quels usages ? Pikcio, un Pims pour agréger et partager ses données

Pikcio utilise le réseau de MatchUpBox. C'est un service qui permet d'échanger de façon sécurisée. Le serveur de données est sur les machines des utilisateurs donc tout ce qu'ils peuvent échanger au sein de ce réseau est sur leurs machines. Il existe ensuite des API

pour se connecter au réseau MatchUpBox.

“Pikcio est une plateforme de services intelligente. Elle utilise le réseau propriétaire MatchUpBox, de type Blockchain. Pikcio centralise des données de différentes sources (compte personnel ameli.fr, centres de soins, dossier médical partagé…) et de différents types (santé, identité, banque, assurance, etc.) pour faciliter et protéger les échanges entre consommateurs, médecins et établissements de santé.”

L’ambition de Pikcio est de devenir un Pims (Personal Information Management System) : un espace d’agrégation des données de l’individu, aujourd’hui éparpillées dans différents services.

Pourquoi cette ambition ? Parce que le grand problème du P2P est l’usurpation d’identité, la validation de l’identité sur le réseau (pour reprendre l’exemple précédent : comment justifier que c’est bien Arthur qui me demande comme ami et pas quelqu’un d’autre ?). L’objectif premier était donc de récupérer des données éparpillées par l’individu et d’en faire l’analyse pour donner un indice de confiance aux profils utilisateurs.

En faisant ça, on permettait à l’individu de récupérer beaucoup de données : les données Facebook, les données Twitter etc. Récupérer de la donnée pour permettre de vérifier l’identité d’un utilisateur c’est bien, en faire d’autres choses, c’est encore mieux ! Un travail est réalisé en ce moment pour permettre aux utilisateurs d’agréger des données de différentes sources. Par exemple un travail avec les API de Qwant. Mais cela doit se faire toujours sous le contrôle de l’individu, qui doit être le déclencheur de cette agrégation.

Retrouver la présentation de Jorick Lartigau ici.

Quatre interventions, quatre visions du Self Data qui se rejoignent dans les principes, dans les enjeux et qui démontrent que si les pistes techniques sont là en terme d’architecture, de stockage, de moyen d’identification/d’authentification ou d’agrégation des données, elles doivent encore être discutées, unifiées pour s’articuler et permettre à ce nouveau marché du Self Data de se développer.

Merci à tous les participants de cette rencontre, et retrouvez-nous pour la prochaine des Rencontres du Self Data le 22 février après-midi pour un moment d’échange sur les défis juridiques du Self Data !

Article importé:
http://mesinfos.fing.org/les-rencontres-du-self-data-les-architectures-et-defis-techniques-du-self-data/?utm_source=rss&utm_medium=rss&utm_campaign=les-rencontres-du-self-data-les-architectures-et-defis-techniques-du-self-data
Par: Manon Molins
Publié: February 7, 2017, 7:36 am