Verbatim de la conférence donnée à l'Université de Caen lors la journée du pôle TES

le 14 Novembre 2017 par Pierre Gradit, mezzonomy.

[1]

Bonjour à tous et à toutes, le sujet de cette keynote est "*la blockchain est-elle bonne pour la santé*".

[2]

Pour les plus anciens d'entre nous, le titre de cette planche vous fera penser au slogan de SUN MICROSYSTEMS, "*the network is the computer*".

La blockchain réalise ce programme en un nouveau paradigme qui transforme un réseau de machines communicantes en une seule super-machine (intriquée).

Une machine, par exemple, un smartphone, héberge un système d'exploitation (android), des applications (téléphone) et des fichiers (contacts).

Dans la première blockchain, tout s'appele "*bitcoin*", le système d'exploitation, l'application et le registre (Cela n'aide pas à comprendre). Et d'ailleurs avant 2013, son exposition demeure confidentielle.

En 2013, Vitalik Buterin crée Ethereum, et différencie les différents éléments, avec une pluralité d'applications. Y subsiste que le système et le registre sont, peu ou prou, le même objet, la blockchain – un terme absent du célèbre article définissant bitcoin.

Notre blockchain, mezzonomy, est un système multi-registre qui n'est pas une crypto-monnaie.

[3]

Qu'est ce que la "*blockchain*" ?

(et plus généralement les "*Decentralized Ledger Technologies*")

C'est un registre commun inaltérable

- identique partout, sur toutes les machine du réseau

- vérifiable par toutes les machines du eéseau

- utilisable par toutes les machines du réseau

Vérification et utilisation se réfèrent à un agrément qui définit les "*règles de la blockchain*". Par exemple, pour dépenser une somme en bitcoin, je dois prouver que je la possède (Bitcoin ne fait pas crédit, ce n'est pas une banque). C'est une règle. L'ensemble des règles forment l'agrément d'usage de la blockchain.

Comment la blockchain fonctionne-t-elle ? Comment arrive-t-elle à faire qu'un réseau de machine se comporte comme une seule machine avec un seul état ? Grâce à une innovation cryptographique mise au point dans les années 90 et finalisée dans les années 2000, qui est une sorte de "*compression aléatoire*".

N'importe que fichier (voire même tout votre disque dur) peut être compressé en un temps très court en un seul mot de 256 bit de données.

Et deux compressions différentes auront des résultats différents

(en pratique)

Car les mathématiques vous disent que vous aurez une chance sur 2^{256} que deux compressions aléatoires différentes mènent au même résultat.

Le truc c'est que 2^{256} est un nombre défiant l'imagination.

Donc si je vous dit 2^{256}, et bien c'est pour le moins abstrait (cela défie l'imagination).

En revanche, si je vous dis que 120 milliards de dollars sont dans un coffre conçu de cette façon et que personne ne l'a forcé, c'est déjà plus concret.

C'est en cela que bitcoin (dont la capitalisation est de 120 G$) est la preuve que la blockchain fonctionne.

Car ce qui est étrange dans ce nouveau paradigme qui intrique toute les machines en une seule, c'est qu'il intrique aussi des concepts qui n'appartiennent pas au fond classique de l'informatique, mais plus au champ juridique : le temps, la preuve et la confiance.

Le temps, en effet, car une blockchain sédimente l'information, comme on parle de "registre fosssile" pour dire qu'un strate sous une autre est toujours plus ancienne.

La preuve car la compression sert de preuve d'existence d'une donnée, quelle que soit sa taille.

Et la confiance, parce que le registre crée de la confiance. La plus ancienne oeuvre d'art que nous comprenons, le "*scribe accroupi*" représente un homme en train de tenir un registre.

Cette confiance traverse le temps.

[4]

Maintenant, si nous regardons le monde de la santé en empruntant la voie réglementaire, nous pouvons partir de "l'évolution des systèmes de santé"

Et si nous regardons les concepts de temps, de preuve et de confiance, nous pouvons les associer à des éléments saillants de ce programme.

Au temps, nous pouvons associer l'idée de parcours, et singulièrment l'idée de "*parcours patient personnalisé*"

A la preuve, nous allons associer toutes les problématiques de la certification et de la conformité des processus.

Enfin, à la confiance, nous allons pouvoir associer la notion de "*mise en commun des moyens*" (la blockchain est toujours une mise en commun de données).

Nous voyons que cela se présente plutôt bien (nous avons un bon "*match*").

[5]

Pour aller plus loin et dépasser ce constat positif, mezzonomy est impliqué dans le projet BPVS avec PolePharma et HighFi : "*Blockchain Pharma pour le Val de Seine*".

L'objectif est d'identifier les "*usages des registres blockchain pour les réseaux de santé*".

La coloration pharamceutique n'impacte guère la mise en commun et la conformité (ce sont les mêmes problèmes ici ou là).

En revanche, au parcours du patient, nous pouvons ajouter le parcours des substances, depuis la collecte ou la synthèse des principes actifs jusqu'à l'administration au patient.

(pour ne citer que les sujets que nous avons déjà explorés dans l'ecosystème de mezzonomy)

Ces usages autour du parcours des substances vont des questions de logistique, comme celle des douanes, jusqu'à celle de la iatrogénie,

[6]

Alors quels sont les challenges que doit dépasser la blockchain pour être utilisée dans

le contexte de la santé et plus généralement dans tout contexte industriel.

D'abord celle du "*coût énergétique*". Nous l'avons vu, bitcoin devient un phénomène financier significatif en gérant 0.05% de la richesse mondiale (120G$). Mais c'est aussi un phénomène énergétique qui consomme 0.13% de la production électrique mondiale. Pour un registre qui ne fait "*que*" 180Go. Un tel système ne peut pas être généralisé à une fraction significative des données mondiales.

Il faut comprendre ici que c'est parce que bitcoin est une blockchain publique à preuve de travail, et qu'il existe d'autres modes d'utilisation de la blockchain et d'autres systèmes de preuves (preuve d'implication, preuve de process). Cette question est activement étudié, et si tout ici est encore buissonnant, il existera dans un proche avenir, pour toute situation donnée, des solutions qui feront consensus.

Vient ensuite la question de la conformité avec la réglementation, sur les données personnelle par exemple, ou plus récemment la question soulevée par la CNIL du droit à l'oubli (ce qui pour lablockchain revient à pointer où cela peut faire souffrir). Encore une fois, des solutions existent pour cette question, mais je n'ai pas le temps de les développer ici

[*ce sera fait lors de la table ronde avec le concept de* "registre personnel de recoupement" *ou* "registre sans données" *servant seulment à désigner des séquences de faits autonomes comme relevant de la même personne à la manière d'un wallet bitcoin*]

Une question plus brûlante, celle de l'évolution des agréments. Cela porte le doux nom de "*fork*" et c'est la plaie des crypto-monnaies. Il faut savoir qu'aujourd'hui, vous avez deux bitcoins (cash) et deux ethereum (classic). Pour un truc qui est censé durer une éternité, il est permis de se demander combien y en aura-t-il dans vingt ans à cette cadence :-)

Ceci est une question très épineuse, et je vous présenterai plus tard la solution que mezzonomy apporte à ce problème.

Enfin, principal frein au déploiment de systèmes blockchains, la question de leur cohabitation avec les systèmes existants. En effet, les notions d'identité, de temps et de preuve sont beaucoup plus friables dans les systèmes existants, et une blockchain aurait tendance à n'avoir aucune confiance dans de telles interactions.

Pour arriver à les faire cohabiter, il faut rajouter de l'intelligence (artificielle ?) à l'interface entre les deux types de machines pour que la blockchain puisse avoir confiance. Cet ajout porte le nom d'oracle.

(et c'est tout un programme)

[7]

Alors dans ce contexte, quels sont les savoir-faire de mezzonomy.

C'est d'abord un boîte à outil pour faire vivre des registres dans des ecosystème métiers.

Car mezzonomy est d'abord une blockchain multi-registre (qui n'est pas une crypto-monnaie) et nous avons la conviction (étayée) que la plupart des situations réelles nécessitent plusieurs registres.

Notre plate-forme est intégrée au web de façon native, nous parlons XML, REST, WebSockets, XSL, javascript, bref nous parlons développement web

Enfin, et c'est une application essentiel de la capacité multi-registre, nos agrément sont dynamiques, négociés et certifiés, car un agrément provient de l'activité sur un autre registre que celui qu'il régule.

Nous récupérons ainsi au niveau de l'agrément toute la profondeur du temps, de la preuve et de la confiance blockchain, et ainsi nous n'avons pas de "*fork*".

Je vous remercie de votre attention.