beAchain : une société numérique villageoise

Dans un village tout le monde sait tout sur tout le monde. Ça a un côté exaspérant mais aussi un côté rassurant : cela garantit que toute transaction - un mariage, un divorce, la cession d'une terre, le legs d'une maison, la location d'une machine agricole, le vote pour le président de l'association locale sportive - se fera non seulement au vu et au su de tous, mais aussi que les acteurs et les termes de la transaction sont connus de tout le monde. «On» sait que Georges a vendu un bout de son champ à Julien. Quand Georges et Julien ont négocié la vente, si ils ont eu Xavier, Marie, Bernard et sa cousine Léa comme témoins vous pouvez être sûr qu'en quelques heures tout le village l'a appris.

Si un jour un certain Robert essaie de faire croire que ce bout de terrain est en fait à lui, il n'y a ni besoin d'aller chez le notaire ni au cadastre ni chez le juge ni chez l'avocat… il suffit de demander à n'importe que habitant du village à qui appartient le bout de champ qui va de la route au petit bois pour le savoir. C'est rapide, efficace et économique. Et surtout imparable : personne ne peut ni modifier ni détruire cette information détenue par tous qui dit que le bout de champ appartient bien maintenant à Julien. Il suffit donc pour n'importe quelle transaction de quelques témoins qui vont tout aller raconter aux autres - qui, quel jour, à quelle heure, pourquoi, comment, combien… - pour qu'elle devienne *inaltérable, inattaquable et irrécusable*. Sauf que. Sauf que si une moitié du village décide de s'allier contre Julien et essaie de faire croire à tout le monde que le champ est bien à Robert hé bien c'est la pagaille. Alors comment faire ?

Tout l'intérêt des villages est que *si tout le monde sait quelque chose, tout le monde ne sait pas tout*… Fred saura que Jules a été à telle école mais pas qu'il avait redoublé sa cinquième ; Jules saura que Benoît est le cousin de Noémie mais pas que Françoise est sa maman ; Noémie saura que Fred est sorti avec Chloé mais pas que Jules aussi… Bref, il y a dans notre village tout une collection de micro-savoirs qui, si on parvenait à les réunir tous ensemble, formeraient *l'intégralité de tout ce qui se sait sur tout* ; il suffirait dès lors de comparer «ce que sait réellement chacun» avec «ce que tous savent virtuellement» pour *déterminer si n'importe quelle affirmation est vraie, fiable et conforme* à ce qui serait dit si tout le monde savait tout. Robert n'aurait alors aucune chance de se faire passer frauduleusement pour le propriétaire du champ ; ce ne serait même pas la peine d'essayer tant la manoeuvre est perdue d'avance.

Donc si l'on pouvait disposer dans chaque village d'un dispositif permettant, dès lorsqu'une transaction est engagée, de comparer ce que les uns et les autres savent alors on parviendrait à *établir une confiance absolue en chaque acteur et pour chaque transaction*. Si par exemple Albert me vend dix kilos de pommes bio, je suis sûr et certain que (1) le verger lui appartient, (2) les pommes viennent bien de chez lui, (3) il n'a jamais déversé de produits chimiques sur ses arbres. Je le sais et j'ai confiance parce que *tout le village détient en commun les informations nécessaires à s'en assurer* : si le verger n'était pas à lui, ou si il y déversait des pesticides à la tonne, ou si il s'était fait livré des pommes d'Espagne par camion, ou même si il n'était pas Albert mais un escroc se faisant passer pour lui, il est absolument certain que plus de la moitié du village le saurait. La transaction frauduleuse serait alors immédiatement annulée.

Imaginons maintenant un certain Bob qui arrive dans notre village ; il ne connaît personne et cherche la maison d'une certaine Alice, une amie qui l'a invité à venir passer le week-end dans sa maison de campagne. Il demande à un promeneur où se trouve la maison d'Alice. Que fera ce dernier si il ne sait pas ? …il appellera quelqu'un qui pourrait le savoir, par exemple l'épicier devant sa boutique. Toi tu sais où habite une certaine Alice ? L'autre cherche dans sa mémoire mais ne trouve pas ; une dame qui faisait ses courses intervient : ce ne serait pas par hasard la Alice qui a repris la maison de ses grands-parents à la sortie du village ? Bob confirme que oui, que c'est sûrement elle. L'épicier répond que bon, si c'est une étrangère il est possible qu'il ne la connaisse pas ; la dame insiste : mais si c'est la fille à Bernard, tu sais le fils de Louis et de Madeleine. Ah oui elle !, hé bien je ne savais pas qu'elle s'appelait Alice. Bob s'éloigne et le buraliste qui avait assisté à la scène vient demander ce qui se passe. Il cherchait quoi ce type ? La maison d'une certaine Alice, la fille du fiston de Louis. Ah bon, Louis avait un fils ? Oui mais il est parti très jeune faire des études à la ville, il ne revenait presque jamais au village, tu ne l'as peut-être pas connu… Le soir à table, le buraliste raconte l'histoire d'Alice à son épouse qui elle-même etc. Fin de l'histoire.

Que s'est-il exactement passé ? Excepté Bob qui lance la transaction et Alice tout en bout de chaîne comme destinataire, nous avons un certain nombre d'acteurs impliqués à degré ou à un autre dans cette transaction - le promeneur, l'épicier, la dame, le buraliste, l'épouse - qui détiennent tous plus ou moins d'informations. C'est en échangeant les uns avec les autres qu'ils parviennent non seulement à valider la transaction - Bob sait maintenant où est Alice - mais aussi à enrichir et mettre à jour dynamiquement leurs propres informations. A partir de l'épouse le schéma se modifie : ce ne sont plus des *acteurs directs qui échangent et valident leurs savoirs de façon bi-directionnelle* mais de la *distribution unidirectionnelle d'information* - l'épouse à sa voisine, la voisine au facteur, le facteur à la postière, la postière au retraité. Ainsi, par capillarité, l'information «Alice fille de Bernard fils de Louis et de Madeleine habite la maison et y invite des gens le week-end, je le sais d'untel et d'unetelle» finit-elle par se diffuser de proche en proche, mettant à jour toutes les mémoires individuelles touchées par la vague en même temps qu'elle renforce le savoir commun global.

Une blockchain de village

Les technologies et protocoles assurant le fonctionnement de **beAchain** forment un «village numérique global» dont chaque machine connectée serait habitant. Quand la machine A (celle de Alice) veut verser disons 1000 unités à la machine B (celle de Bob), les plus près de A cherchent dans leurs datas internes - directement dans les blocks cryptés empilés en chains - ce que les unes et les autres savent de A et de B. En comparant leurs données respectives dans de brefs dialogues cryptés elles parviennent (ou pas) à se mettre d'accord entre elles : la transaction est-elle *valide, faisable et acceptable* ? Si le OUI fait consensus, elles mettront alors aussitôt à jour leurs propres datas concernant A, B et celles de leurs comptes respectifs ; en même temps elles autoriseront A et B à se réactualiser mutuellement. Ceci fait, elles initieront un *process par capillarisation de mise à jour des autres machines* par distribution unidirectionnelle : d'abord toutes les machines ayant approuvé la dernière transaction de A et toutes celles ayant approuvé la dernière transaction de B, puis toutes celles ayant un rapport direct d'approbation avec chacune de celles-ci seront progressivement mises à jour selon leurs disponibilité sur le réseau. On parvient ainsi à mettre à jour les datas de plusieurs dizaines de machines - voire de centaines - en quelques dizaines de secondes. On a donc bien dans un premier temps l'épicier, la dame, le promeneur et le buraliste qui *dialoguent en direct pour finalement valider/approuver la demande/transaction* de Bob/Alice, puis, dans un second temps, l'épouse qui le dit au facteur, puis la voisine au retraité, puis la postière à etc.

L'approbation consensuelle est quant à elle beaucoup plus rapide : le dialogue comparatif - chaque machine cherche et dit ce qu'elle sait sur A et B - dure de 1 à 4 secondes selon l'état du réseau, la puissance de chaque machine, la disponibilité du processeur, etc. En disons 2.5 secondes en moyenne, 10 machines sont capables d'assurer un consensus fiable et sûr sur une seule transaction à la fois. Mais notre «village numérique» ne compte pas 10 habitants mais 1000 ; pendant que 10 sont occupés à gérer une transaction en cours, les 990 autres peuvent donc gérer 99 autres transactions simultanées. Une transaction durant 2.5 secondes, en 1 seule seconde on peut donc gérer 100 / 2.5 soit 40 transactions simultanées ; avec seulement 5 approbateurs/validateurs au lieu de 10, et avec 100 000 machines connectées, on gère donc jusqu'à 8 000 transactions/seconde.

En comparaison, d'autre solutions blockchain concurrentes peuvent mettre jusqu'à plusieurs minutes pour approuver une seule transaction. D'autres, plus rapides, parviennent à un résultat de 1 transaction toutes les 4 secondes. Pourquoi cette différence avec **beAchain** ? Parce que là où **beAchain**, blockchain orientée objets, pense en logique de «machines sociales» organisées comme un village, d'autres blockchains pensent en logiques urbaines verticales où de parfaits inconnus ne sachant rien les uns des autres doivent apprendre à se faire confiance et, n'y arrivant pas, sont obligés de remonter le fil du pourquoi du comment de chaque information qu'ils ont à traiter. Assurer à la fois la *fiabilité, l'infalsifiabilité et l'indestructibilité* de l'information est la base de tous les protocoles blockchain. Comment y parvenir - à quelle vitesse, à quel coût, à quelle fréquence ? - les distingue les unes des autres. **beAchain** et ses «machines sociales» propose une solution dynamique, puissante et rapide apte à répondre à de nombreux cas d'usages dans des domaines aussi différents que la transaction financière, l'échange instantané de date entre objets connectés ou la prise de décision par des outils d'intelligence artificielle.

BEACHAIN

ab@beachain.com / www.beachain.com