

HOMO SAPIENS INFORMATICUS chronique de Gilles Dowek

Jusqu'où ira la révolution « blockchains » ?

Les chaînes de blocs sont un moyen nouveau de conserver de l'information de manière sécurisée. Ce système va probablement changer le monde dans lequel nous vivons...



Quand nous achetons par exemple un appartement, nous souhaitons pouvoir prouver, des années plus tard, que nous en sommes propriétaire, au cas où Dame Belette y porterait frauduleusement ses pénates. Pour ce faire, nous utilisons un procédé qui remonte à la fin du XVII^e siècle : tous les actes de vente et d'achat sont inscrits dans un grand registre, le « fichier immobilier », conservé par un service de l'État, le service de publicité foncière, auquel les notaires communiquent, à chaque signature, les actes à conserver.

Dans ce procédé pour conserver de l'information, un site, le lieu de conservation du registre, joue un rôle particulier. Cette centralisation fragilise l'information, qui pourrait disparaître si un incendie détruisait ce registre, et elle rend difficile le passage à l'échelle : ce procédé ne fonctionnerait peut-être plus si le nombre d'actes de vente et d'achat était soudain multiplié par mille ou par un million. C'est pourquoi *Homo sapiens informaticus* lui en préfère un autre : au lieu de communiquer au service de publicité foncière les actes à conserver, chaque notaire conserve lui-même une copie du fichier immobilier et les notaires s'informent les uns les autres des actes à y inscrire. Ce procédé n'utilise pas de fichier centralisé et l'État n'y joue aucun rôle.

Il se peut cependant qu'un notaire maladroite ou malhonnête ait, dans sa copie du fichier, une information différente de ses collègues. Pour éviter ces erreurs et ces fraudes, l'information détenue par plusieurs notaires prime sur celle détenue par ce seul notaire.

Cette organisation est la base des systèmes informatiques de « chaînes de blocs » (*blockchains* en anglais), où des notaires – des programmes répartis sur de nombreux ordinateurs – tiennent des registres – des bases de données – et les synchronisent en permanence. En cas de désaccord entre deux programmes, l'information majoritaire prime.



LE BITCOIN EST UNE MONNAIE virtuelle fondée sur des registres de type chaînes de blocs.

Un tel système est relativement fiable : il faudrait une coalition d'une majorité de notaires pour organiser une fraude. Cependant, comme ces notaires ne sont que des programmes dans les chaînes de blocs, créer un notaire n'est pas difficile et un fraudeur pourrait facilement créer des milliers de notaires, afin de constituer une majorité. Pour parer de telles attaques, les chaînes de blocs font « payer » les notaires, en temps de calcul par exemple. Les notaires doivent ainsi, pour participer à une chaîne, effectuer des calculs inutiles, une activité nommée minage. Ainsi, créer des milliers de notaires

a un coût élevé en puissance de calcul, ce qui décourage les fraudeurs.

La conservation des actes de propriété n'est pas la seule activité qui serait transformée par le développement des chaînes de blocs. En effet, conserver un registre impossible à modifier frauduleusement est aussi la principale activité des bureaux de vote, des banques, des services du cadastre, etc. Bien entendu, si le contenu de certains de ces registres doit être rendu public, celui d'autres, tel le registre qui consigne quel électeur a voté pour quel candidat, doit être tenu secret.

Cet exemple des chaînes de blocs nous montre que les métiers de facteur ou de conducteur de camion ne sont pas les seuls condamnés à décliner, ou à se transformer radicalement, du fait du développement de l'informatique : les métiers de notaire et de banquier sont tout autant concernés.

Cependant cette transformation n'est peut-être pas l'effet le plus important du développement des chaînes de blocs : comme la conservation du fichier immobilier, la création d'une nouvelle monnaie était naguère un privilège des États. Mais, comme la conservation du fichier immobilier, une monnaie n'est qu'un moyen de conserver de l'information sur la durée : l'information des recettes et dépenses de chacun, ou plus précisément de leur solde. Ainsi, avec les chaînes de blocs, ce privilège de créer une monnaie échappe, lui aussi, aux États. ■

Gilles DOWEK est chercheur à l'Inria et membre du conseil scientifique de la Société informatique de France.

CABINET DE CURIOSITÉS SOCIOLOGIQUES par Gérald Bronner



Les années 1960 et le crépuscule de l'idée de progrès

L'utilisation du mot « progrès » a commencé à décliner alors que l'on était en plein dans les Trente Glorieuses. Pourquoi ?

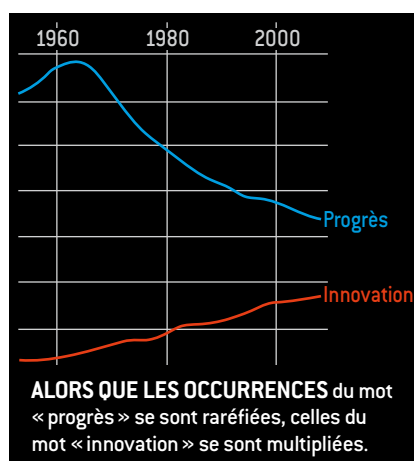
La numérisation massive des livres entreprise par Google depuis 2004 permet de mettre à disposition de tous, via l'application Ngram Viewer, des données essentielles pour répondre à bien des questions. Grâce à cette application, on peut connaître la fréquence relative de l'apparition de tel ou tel terme dans l'immense base de données ainsi constituée (plus de 15 millions d'ouvrages), et donc d'en évaluer une partie de la popularité.

Par exemple, Ngram Viewer offre la possibilité de tester la réalité de la baisse d'audience de certains termes comme celui de « progrès », dont plusieurs penseurs ont estimé qu'il était en déclin. C'est notamment le cas du philosophe français Georges Canguilhem qui, dans un article fameux de 1987 (*Revue de Métaphysique et de Morale*, vol. 92(4), pp. 437-454), proposait une analyse de la décadence du terme « progrès ».

À ce sujet, le physicien et philosophe Étienne Klein livrait récemment une intéressante réflexion : « Le mot progrès est de moins en moins fréquemment utilisé [...]. Il se trouve remplacé par un mot qui n'est pourtant pas son synonyme : innovation. »

Étienne Klein a tout à fait raison de considérer que l'un et l'autre termes ne sont pas substituables. La notion de progrès implique une forme de philosophie de l'histoire qui fait le pari que demain sera préférable à aujourd'hui. Elle constitue un principe collectif mobilisateur qui paraît, en effet, avoir été affaibli et mis en marge de notre horizon commun.

La notion d'innovation est, le plus souvent, positivement connotée, mais elle est perçue, selon Étienne Klein, comme un effort pour remonter la pente que le temps corrompateur nous ferait descendre. Cette substitution dirait donc bien quelque chose d'une mutation de nos représentations collectives. Cependant, comme nous le rappelle sagement Fontenelle : « Assurons-



nous bien du fait, avant de nous inquiéter de la cause. Il est vrai que cette méthode est bien lente pour la plupart des gens, qui courent naturellement à la cause, et passent par-dessus la vérité du fait ; mais enfin nous éviterons le ridicule d'avoir trouvé la cause de ce qui n'est point. »

C'est précisément dans ce registre que le recours à Ngram Viewer est précieux, car on imagine sans peine le temps qu'il eût fallu pour évaluer la fréquence de l'utilisation du terme « progrès » dans la littérature par

comparaison avec celui d'« innovation » et celui, plus important encore, qu'aurait nécessité une comparaison internationale. Observera-t-on la même chose en français et en anglais, en italien ou en allemand ?

Comme le montre le graphique ci-contre, on constate en langue française (et dans la littérature qui a été intégrée dans l'application proposée par Google) une nette inflexion de l'utilisation du terme « progrès » et, corrélativement, un recours non moins net à celui d'« innovation ».

Le plus fascinant est qu'on observe le même phénomène en langue anglaise, italienne, espagnole, allemande ou même russe ! Non moins fascinante est la constatation que, dans toutes les langues, cette inflexion surgit au cours des années 1960 (à l'exception du russe, où elle apparaît au début des années 1980), c'est-à-dire au cœur même des Trente Glorieuses, avant les chocs pétroliers, avant la fin du monde bipolaire ou même avant que la notion de mondialisation devienne une préoccupation généralisée (là aussi, Ngram Viewer permet de constater que le succès du terme date du début des années 1990).

Qu'a-t-il donc bien pu se produire au moment où la majorité des pays développés connaissaient leur plus forte croissance économique et, d'une façon générale, une amélioration considérable de leurs conditions de vie ? Voilà bien un paradoxe que ne permettent pas de résoudre les algorithmes.

Gérald BRONNER est professeur de sociologie à l'université Paris-Diderot.

Désinformation sur Ce que révèlent les statistiques

Walter Quattrociocchi

Les internautes diffusent massivement des informations fausses et des théories conspirationnistes farfelues. Des études statistiques portant sur les réseaux de Facebook apportent un éclairage quantitatif et inédit sur les mécanismes à l'œuvre dans cet inquiétant phénomène.

Ne vous est-il jamais arrivé de dîner avec des amis ou des membres de votre famille et que la conversation tourne autour de rumeurs circulant sur Internet, par exemple sur le rôle des traînées de condensation des avions dans le réchauffement climatique ou sur les avantages de telle ou telle méthode de médecine alternative ? Ou de suivre à la télévision les commentaires de comédiens ou chanteurs célèbres, sans connaissances particulières en économie ou en politique, devenus tout à coup de fins analystes de la situation internationale ?

Qu'est-ce qui a changé dans notre façon de nous informer, et donc de nous forger une opinion ? Quel rôle les médias sociaux tels que Facebook jouent-ils dans la diffusion de fausses informations ou de thèses conspirationnistes ? Quels sont les ressorts de cette mésinformation ou désinformation ? Est-il possible d'endiguer ces phénomènes ?

Comme le montre l'actualité, tant nationale qu'internationale – le Brexit, l'élection de Donald Trump à la présidence des États-Unis, le climat-scepticisme, la radicalisation islamiste de certains jeunes Européens, etc. –, ces questions sont d'importance : elles ont une incidence directe sur

nos sociétés et les grandes orientations (économiques, politiques, etc.) qu'elles se choisissent.

On comprend donc que de nombreux sociologues se soient penchés sur les phénomènes sociaux liés à Internet et à ses médias, et notamment sur la « viralité » des informations infondées ou fausses, c'est-à-dire leur capacité à se propager vite et massivement.

Ils ne sont pas les seuls. Depuis plusieurs années, des mathématiciens, des physiciens, des chercheurs en informatique se sont aussi intéressés à ces problématiques, en apportant leurs propres outils et méthodes d'analyse. Ainsi a émergé, dans les années 2000 à peu près, un nouveau champ de recherche : les « sciences sociales computationnelles ».

Via une approche qui repose sur l'analyse de grandes masses de données, cette discipline s'attache à combiner mathématiques, statistiques, physique, sociologie et informatique, afin d'étudier les phénomènes sociaux de façon quantitative. Il s'agit d'exploiter, grâce à des techniques d'analyse adaptées, les très nombreuses traces numériques que laissent les internautes sur les différents médias sociaux tels que Facebook, Twitter, YouTube, etc. lorsqu'ils sélectionnent,