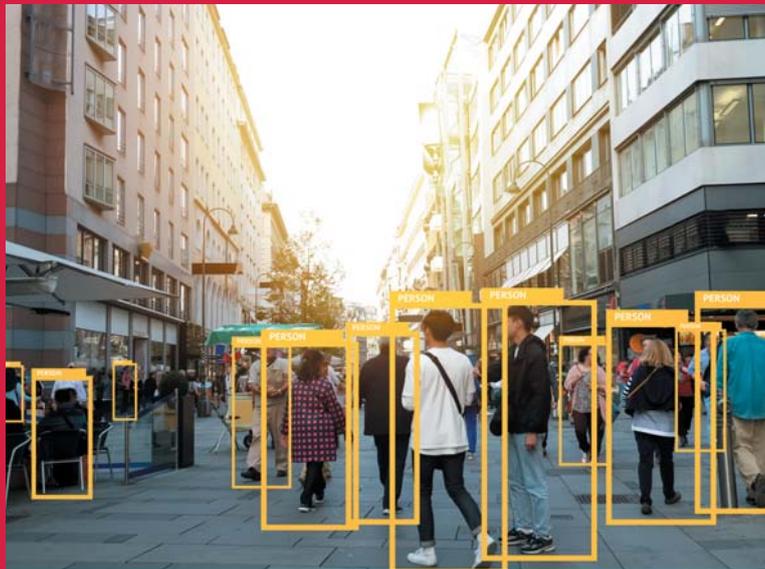


LES *BLOCKCHAINS* ET LE SYSTÈME NERVEUX CITOYEN

Alessandro Voto

Institute for the Future - Blockchain Labs



Alessandro Voto est Directeur régional (côte ouest) de Consensys, une société spécialisée dans les technologies blockchain basée à Brooklyn. Son rôle consiste à relier les organisations et les entrepreneurs sociaux à la communauté locale de la blockchain en vue de créer des applications et des services. Alessandro est également auxiliaire de recherche au Blockchain Futures Lab de l'Institute for the Future.

MOTS CLÉS

- BLOCKCHAIN
- BITCOIN
- CONTRATS INTELLIGENTS
- CRYPTOMONNAIES
- PROTOCOLES AUTONOMES
- IDENTITÉ NUMÉRIQUE
- GESTION MUNICIPALE DÉCENTRALISÉE
- « GOUVERNEMENT EN TANT QUE FOURNISSEUR DE SERVICES »

Dans cet article, Alessandro Voto nous fait découvrir de quelle manière l'essor des protocoles blockchain transformera la gestion des villes. Ils permettent en effet d'imaginer une gouvernance municipale plus répartie et l'émergence d'une nouvelle gamme de services urbains où machines et humains collaborent d'une nouvelle manière pour le stockage, les déplacements et les transactions.

Destinés à fonctionner pour un prix bien plus modique que les protocoles centralisés, ces nouveaux services seront particulièrement adaptés aux populations mal desservies, en leur apportant une identité plus mobile et plus sûre, adaptée à leur création de valeur.

INTRODUCTION

Contrairement au « cerveau » centralisé de la politique traditionnelle de la cité, les systèmes nerveux citoyens basés sur la technologie blockchain distribueront l'intelligence politique et les dynamiques économiques jusqu'en périphérie. Les humains ne seront plus les seuls à prendre des décisions et à agir en conséquence. Les machines et les agents d'intelligence artificielle seront des contributeurs tout aussi impliqués dans la symphonie de la cité intelligente de demain.

La cité est un organisme distribué. Les citoyens travaillent en symbiose pour transformer des matières premières en produits et en services utiles à la vie et à un ensemble plus vaste. Pour déplacer et protéger la valeur qu'ils créent ensemble, ils dépendent d'infrastructures civiles comme les lois, les marchés et les contrats. Ensemble, ces outils et ceux qui les font respecter agissent comme un système nerveux de la cité, et permettent aux communautés de réagir de manière fiable aux besoins émergents et aux attaques éprouvantes.

Jusqu'à présent, nous avons besoin d'un gouvernement central et d'institutions pour gérer les enregistrements et les processus derrière cette infrastructure, à l'échelle de la cité. Nous avons donné à ces institutions le pouvoir de limiter artificiellement nos interactions, afin qu'elles puissent en tirer un bénéfice ou interdire des activités qu'elles jugent inappropriées. Cependant, elles sont devenues des cibles privilégiées des violations de données et des manipulations par des tiers.

Les avancées récentes de la technologie tendent à éliminer le besoin d'une bureaucratie centralisée, en connectant directement les pairs pour les aider à suivre et à exécuter eux-mêmes les accords économiques et sociaux. Une de ces technologies, nommée *blockchain* (chaîne de blocs), utilise ces liens directs comme une protection contre le pouvoir civil centralisé.

Les *blockchains* sont une sorte de base de données partagée qui permet aux communautés de conserver des enregistrements dans un réseau d'ordinateurs. Chaque personne peut soumettre un enregistrement afin que les autres la stockent dans la chaîne chronologique et synchronisée, avec les enregistrements de ses pairs. Les enregistrements et leur séquence sont protégés par un cryptage de qualité bancaire pour empêcher toute modification, suppression ou contrefaçon par un quelconque acteur du réseau.

La technologie des *blockchains* va faciliter de toutes nouvelles formes de coopération dans les cités et entre elles. Elle va étendre les protections institutionnelles dignes de confiance et les services financiers aux personnes marginalisées et démunies dans le monde entier. Elle va réinventer la manière dont nous gérons l'infrastructure physique de la cité et les structures communautaires numériques. La suite de cet article est un aperçu du système nerveux citoyen que les *blockchains* pourraient soutenir à l'avenir.



UNE IDENTITÉ POLYFORME

La participation à la vie de la cité commence avec l'identité et la citoyenneté. Qu'il s'agisse d'une personne, d'une société ou d'un appareil, l'unicité de l'identifiant nous aide à étendre notre confiance aux bons groupes et à nous protéger des acteurs malveillants. Pour cette raison, une des fonctions les plus importantes que peut remplir la *blockchain* est la gestion des informations identitaires des personnes et des organisations.

Aujourd'hui, c'est votre carte d'identité, votre permis de conduire, votre profil dans les réseaux sociaux et d'autres formes d'identité institutionnelle qui permettent de vous identifier. Sans ces éléments, il est difficile ou impossible d'accéder aux services financiers et aux protections légales. Les Nations Unies estiment que 1,5 milliard de personnes dans le monde vivent actuellement sans identité formelle, ce qui les exclut des services urbains et des protections qui en découlent.

Avec des services identitaires basés sur une *blockchain*, toute personne peut établir un identifiant numérique unique à peu de frais. Avec cet identifiant, il devient possible d'associer des données sur ses activités et ses relations, par des transactions *blockchain* successives. Chaque enregistrement supplémentaire, non falsifiable, contribue à affiner l'image de la personne et le degré de confiance qu'elle mérite. Comme toute personne sur le réseau disposant d'une copie de la *blockchain* peut accéder à ces enregistrements, les résidents d'une cité peuvent facilement trouver de nouveaux collaborateurs et tisser des liens avec eux, selon des critères stricts et vérifiables, tout cela sans gestionnaire central des identités.

Les projets *blockchain* tels Uport de ConsenSys et le système d'identité Blockstack Labs vont ouvrir des possibilités entièrement nouvelles pour la gestion des identités. Les écoles et les formateurs émettront des badges infalsifiables pour leurs élèves, qui serviront de micro-accréditation pour de nouveaux lieux et sites d'apprentissage. Les organisations posséderont leurs propres personas *blockchain*, dont l'impact citoyen et environnemental sera visible et analysé par autrui.

“LA CITÉ EST UN ORGANISME DISTRIBUÉ. LES CITOYENS TRAVAILLENT EN SYMBIOSE POUR TRANSFORMER DES MATIÈRES PREMIÈRES EN PRODUITS ET EN SERVICES UTILES À LA VIE ET À UN ENSEMBLE PLUS VASTE. POUR DÉPLACER ET PROTÉGER LA VALEUR QU'ILS CRÉENT ENSEMBLE, ILS DÉPENDENT D'INFRASTRUCTURES CIVILES COMME LES LOIS, LES MARCHÉS ET LES CONTRATS. ENSEMBLE, CES OUTILS ET CEUX QUI LES FONT RESPECTER AGISSENT COMME LE SYSTÈME NERVEUX DE LA CITÉ.”



Même les robots de la cité seront dotés d'une identité permettant de les suivre et de vérifier qu'ils agissent selon les règles et ne dévient pas de leur mission.

La notion de citoyenneté anéantira les obstacles administratifs puisque les transactions *blockchain* révéleront de riches informations sur les contributions des personnes à leur communauté. Avec des applications comme Bitnation, les populations migrantes aujourd'hui vulnérables jouiront d'une « citoyenneté mondiale », affranchie des frontières. Comme les *blockchains* ne réclament pas nécessairement des informations d'identité statiques et formelles pour autoriser une participation qui leur est utile, on pourrait aussi voir des systèmes de gouvernance basés sur une identité minimale et des identifiants à usage unique, qui étendraient l'accès aux services aux personnes très soucieuses de leur sécurité et du respect de leur vie privée.

Que ce soit par l'intermédiaire d'identifiants riches et souverains ou de personas temporaires, l'identité gérée par *blockchain* permettra à chacun de véritablement posséder ses données et, c'est important, à ses richesses.

DES RÉSEAUX CITOYENS DE VALEURS

Le bitcoin est une monnaie numérique qui a introduit le concept de *blockchain* et qui est devenue sa première application à succès. L'offre de cette monnaie est définie par le logiciel : les bitcoins sont créés au profit des « mineurs » qui utilisent leur ordinateur personnel

pour traiter de nouvelles transactions pour le réseau. Une fois qu'un bitcoin est miné, son propriétaire peut le faire circuler en soumettant aux mineurs un enregistrement de transaction afin qu'il soit inclus dans la *blockchain* publique. Tout cela sans identité formelle et en utilisant uniquement des adresses cryptographiques pour conserver et déplacer les fonds. Les transactions étant enregistrées dans un réseau massif de pairs identifiés par pseudonyme, et non par un processeur central des paiements, toute personne disposant d'une connexion à Internet peut accepter ou transférer la monnaie sans craindre de censure ou des intermédiaires parasites.

Le bitcoin et les autres cryptomonnaies vont déclencher des flux de valeur entre les citoyens et des partenaires mondiaux qui remettent en question les frontières et les réglementations classiques. Les pauvres du monde, aussi bien que son élite, utiliseront ces réseaux sans frottement pour accéder aux offres d'investissement international et aux services bancaires qui leur étaient jusqu'à présent refusés.

Comme il est possible de remonter tous les paiements jusqu'aux comptes émetteurs, les personnes et les organisations choisiront d'associer leur identité « réelle » à leurs comptes, afin d'être reconnues comme le payeur. Les gestionnaires de la cité auront leurs propres comptes, nommés portefeuilles dans le jargon des *blockchains*. Les citoyens verseront des contributions à ces portefeuilles de la cité, de manière transparente, autoriseront collectivement les dépenses, et surveilleront soigneusement les registres de transactions pour minimiser la corruption et le gâchis d'argent public. Les ONG feront de même avec des outils tels que Bitgive, pour aider les philanthropes à suivre l'effet de leur don sur le développement qu'ils veulent favoriser.

Depuis Bitcoin, les développeurs ont produit de nombreuses cryptomonnaies similaires. Dogecoin, par exemple, est une monnaie sur mesure qui a tiré son succès de sa marque ludique caractérisée par des chiens Shiba Inu et de mauvaises traductions. D'autres ont renforcé une volonté de souveraineté financière, comme celle de la tribu des Sioux qui a créé sa propre

cryptomonnaie nommée Mazacoin. Dans les cités du futur, les personnes conserveront leur richesse au moyen d'un grand nombre de jetons, avec leurs propres règles transactionnelles, actifs garants et connexions communautaires. Certains seront totalement fongibles pour encourager l'investissement massif, d'autres seront limités à certaines utilisations.

Les projets émettront des jetons pour suivre les contributions des personnes aux pools de ressources et contribuer à mesurer les accès à ces derniers. La'Zooz, une app de covoiturage basée sur une *blockchain*, fournit, aux conducteurs qui proposent des trajets, des jetons échangeables contre les trajets proposés par d'autres conducteurs. Transactive Grid, Solar Coin et la fondation Energy Web sont trois projets qui visent à créer des microréseaux d'énergie renouvelable, où les voisins se payent mutuellement pour les électrons échangés, sans passer par un fournisseur central d'électricité.

Bien que la sécurité des premières *blockchains* d'aujourd'hui nécessite l'attente d'une confirmation par le réseau, de nouveaux développements dans ce domaine permettront bientôt des transactions hors ligne rapides comme l'éclair, et auront recours au grand réseau uniquement lorsque c'est nécessaire. Cette technique, nommée canal de paiement, autorisera des flux de micropaiements générant peu ou aucun frais de transaction. Cela signifie qu'un internaute peut payer le propriétaire du routeur Wi-Fi qu'il utilise à hauteur des octets qu'il a échangés. Les pollueurs pourraient payer à hauteur de leurs émissions carbonées. Les muralistes pourraient recevoir des dons en rapport avec le comportement des visiteurs dont on suivrait le regard.

Les flux financiers à bas coût faciliteront aussi le financement citoyen, ce qui transformera la forme de la cité à l'aide des citoyens. Avec une capitalisation boursière totale croissante, de plus de 80 milliards de dollars en mai 2017, il existera bientôt une grande quantité de liquidités disponible sans frottement. Partant de ce fait, une société d'investissements immobiliers sur *blockchain* nommée FOAM imagine un monde où les architectes pourraient proposer de nouveaux projets immobiliers comme une campagne Kickstarter, puis permettraient aisément à des investisseurs de tous horizons de devenir actionnaire dans leur production. Les investisseurs et d'autres participants pourraient ensuite voter sur des sujets liés au projet, ce qui ferait de chaque projet une expérience de prise de décision ancrée directement dans sa structure. Cela nous amène à notre prochaine *blockchain*.

UNE CITÉ INTELLIGENTE DISTRIBUÉE

Contrairement au « cerveau » centralisé de la politique traditionnelle de la cité, les systèmes nerveux citoyens basé sur les *blockchains* distribueront l'intelligence politique et les bureaux économiques jusqu'en périphérie. Les personnes ne seront plus les seules à prendre des décisions et à agir en conséquence. Les machines et les agents d'intelligence artificielle seront d'égaux contributeurs à la symphonie de la cité intelligente du futur.

Pour maîtriser la crédibilité de la sécurité dans un contexte de cité intelligente, les développeurs traiteront plus que des informations statiques et des registres d'actifs en *blockchains*. Ils enregistreront aussi des bits de code nommés contrats intelligents, destinés à exécuter des opérations complexes sans dépendre d'un tiers unique. Inventés par le juriste Nick Szabo en 1994 puis mis en œuvre au moyen d'un protocole *blockchain* nommé Ethereum, les contrats intelligents agissent comme un agent fiduciaire et notaire robotisé, auquel les personnes peuvent envoyer des actifs et des données s'ils approuvent les termes du contrat. Personne ne peut changer l'accord, ni empêcher des personnes d'interagir avec lui, ni empêcher son exécution, sauf si c'est explicitement spécifié dans le code lui-même.

“POUR MAÎTRISER LA CRÉDIBILITÉ DE LA SÉCURITÉ DANS UN CONTEXTE DE CITÉ INTELLIGENTE, LES DÉVELOPPEURS TRAITERONT PLUS QUE DES INFORMATIONS STATIQUES ET DES REGISTRES D'ACTIFS EN BLOCKCHAIN. ILS ENREGISTRERONT AUSSI DES BITS DE CODE NOMMÉS CONTRATS INTELLIGENTS, DESTINÉS À EXÉCUTER DES OPÉRATIONS COMPLEXES SANS DÉPENDRE D'UN TIERS UNIQUE.”

Avec cette nouvelle fonction puissante, les cités peuvent remplacer les processus bureaucratiques laborieux par des applications décentralisées, transparentes et efficaces. Nous verrons des droits fonciers, des accords commerciaux, des documents constitutifs, des systèmes de scrutin etc. réinventés de manière à être auto-exécutoires, ce qui libérera des opérateurs coûteux et ouvrira de nouvelles possibilités de collaboration dont l'organisation aurait sinon été onéreuse. Le site d'Ethereum propose même un tutoriel facile à suivre : « comment construire une démocratie sur les *blockchains* », y compris les processus de vote, de gestion des membres et de contrôle des actifs. Lorsque les cités expérimentent de tels outils de gouvernance simples, elles partagent leurs bonnes pratiques sous la forme d'applications « service de gouvernance » en source ouverte.

Les machines concluront des contrats intelligents avec les humains, et ne se contenteront plus d'exécuter le code ; elles décideront même du moment et de la manière d'investir la richesse qui leur est allouée ou d'accepter opportunément une mission. Filament, une société basée à Reno (Nevada) et active dans les *blockchains*, crée déjà des puces intégrables de mise en réseau maillé, permettant aux machines de s'acheter mutuellement du temps et des ressources via des contrats intelligents, dans des environnements ruraux et urbains. Les machines pourraient un jour être « propriétaires d'elles-mêmes », et s'ouvriraient à l'investissement de capital et aux informations provenant des personnes et des bots (programmes automatisés) uniquement lorsque c'est nécessaire à l'accomplissement des missions pour lesquelles elles ont été créées.

La technologie des *blockchains* possède un potentiel immense pour réinventer la manière dont nous construisons la cité, la gérons et faisons des affaires en son sein et d'une cité à l'autre. Ces systèmes citoyens impossibles à arrêter devront être conçus en gardant à l'esprit les besoins humains, pour éviter que l'utilisation des *blockchains* renforce les anciens modèles d'injustice. Un nouveau système nerveux citoyen est sur le point d'éclorre, et c'est à nous de lui enseigner l'avenir que nous souhaitons.