

**Aux représentantes  
et représentants des médias**

## **COMMUNIQUÉ DE PRESSE**

### **Des contrats intelligents adaptés à l'industrie 4.0**

**Neuchâtel, le 27 mai 2021. L'Université de Neuchâtel a démontré la faisabilité de contrats intelligents confidentiels qui pourraient intéresser les fabricants d'objets connectés. Révélé dans le cadre du projet européen LEGaTO visant à augmenter la sécurité et l'efficacité des réseaux informatiques, ce constat constitue un progrès supplémentaire en matière de confidentialité dans les technologies impliquant la blockchain, qui est également à la base des cryptomonnaies.**

Pourquoi les industries, et en particulier les fabricants d'objets connectés, hésitent-elles à explorer les nouvelles opportunités de contrats intelligents (ou *smart contracts*) liées à la technologie de la blockchain ? C'est une question de confidentialité, répond Christian Göttel, qui entreprend un doctorat en informatique sur le sujet, sous la direction de Pascal Felber, directeur de la Chaire des systèmes complexes à l'Université de Neuchâtel. Il l'explique dans une récente chronique du blog du LexTech Institute de cette même université.

Son travail de thèse s'inscrit dans la mise au point de contrats intelligents confidentiels, ce qui diffère de l'esprit de la blockchain « traditionnelle » (comme celle qui gère l'échange de bitcoins) et qui a pour objectif la transparence des transactions (voir encadré). « Car le désavantage de ces implémentations est qu'elles ne garantissent aucune confidentialité pour protéger les données traitées, relève Christian Göttel. C'est-à-dire que les actifs et les interactions commerciales ou le contrat lui-même ne sont pas protégés. De nouvelles technologies sont en développement pour permettre de surmonter ces obstacles. »

Pour y parvenir, la Chaire de systèmes complexes de l'Université de Neuchâtel a collaboré au projet européen LEGaTO, dont le résultat a débouché sur le prototype TZ4Fabric. Ce programme informatique réalisé à l'Université de Neuchâtel permet d'exécuter des contrats intelligents confidentiels destinés en particulier aux appareils mobiles et aux objets connectés. Et ceci, avec une efficacité énergétique supérieure à celle qu'exigent actuellement les réseaux de cryptomonnaies comme le bitcoin ou l'ethereum, très gourmands en énergie électrique.

Mais à quoi peuvent bien servir concrètement ces contrats intelligents confidentiels ? Prenons le domaine de la santé et imaginons un logiciel capable d'apprendre à détecter des états précancéreux. « Pour pouvoir générer ces modèles, il faut énormément de données (comme des images de tissus) qu'on trouve distribuées et stockées dans différents hôpitaux à l'échelle nationale ou internationale », illustre Christian Göttel. Les contrats intelligents confidentiels permettent d'accéder à ces données de manière sécurisée, tout en respectant les lois nationales et internationales sur les données personnelles.

Mais on peut aussi avoir recours à des contrats intelligents pour vérifier le respect des conditions de livraison d'un produit sensible (un médicament ou un produit chimique) qui ne doit pas être exposé à une humidité ou une température excessive tout au long de la chaîne de distribution. Le fournisseur et le client passent alors par des contrats intelligents pour s'assurer que cette clause a bien été respectée, grâce à des capteurs qui testent ces paramètres via la technologie des objets connectés. Au moment où le produit arrive chez le client, le contrat décide, en fonction des conditions de transport enregistrées, de déclencher ou non le paiement de la livraison.

« Avec l'introduction des *smart contracts* confidentiels, les entreprises ont de nouvelles possibilités avec des garanties de sécurité supplémentaires par rapport aux technologies actuelles, conclut le doctorant. Quant à savoir si le statut juridique des *smart contracts* (confidentiels) sera reconnu au niveau mondial de manière à permettre de nouvelles relations commerciales numériques nationales et internationales, cette question reste pour l'heure ouverte. »

Encadré

### **La blockchain en deux mots**

Toute transaction importante (que ce soit l'échange d'argent ou la signature d'un contrat entre deux partenaires) doit nécessiter la validation par un tiers. Dans le monde physique, cela peut être une banque, un avocat ou un notaire. Dans le monde de la blockchain, la transaction s'inscrit dans un immense registre (la blockchain ou chaîne de blocs), sur une ligne de code comprenant la date, le montant qui a transité ou la nature du contrat, l'adresse IP cryptée de l'émetteur et du destinataire de la transaction.

La validation est garantie par le fait que chaque machine impliquée dans au moins une transaction du registre (les participants à la blockchain) reçoit une copie de l'ensemble du registre, ainsi que les lignes de transactions suivantes à mesure qu'elles sont validées. La preuve que la transaction a bien eu lieu repose sur le partage de l'immense registre : c'est donc un système de validation décentralisé, en lieu et place de l'intervention d'un tiers – centralisée – (comme une banque, un avocat ou un notaire).

En savoir plus :

Sur les contrats intelligents confidentiels

<https://www.lextechinstitute.ch/les-smart-contracts-confidentiels-pour-lindustrie-4-0/>

Sur le projet européen LEGaTO

<https://legato-project.eu/>

### **Contact**

*Christian Göttel, Chaire de systèmes complexes*

*Tél. +41 32 718 27 34 ; christian.goettel@unine.ch*