Le CNRS et Télécom ParisTech explorent une monnaie quantique

2018 sera-t-elle l'année de **l'informatique quantique** ? Des passerelles sont en train d'être érigées avec les **monnaies**.

Enfermée dans le secret des laboratoires depuis plusieurs années, l'informatique quantique commence à s'exposer au travers des innovations d'IBM (IBM Q Lab), d'Atos, de Google, d'Intel (Tangle Lake) ou encore de Microsoft (Q#, travaux sur le fermion de Majorana).

Et l'on évoque de plus en plus régulièrement ses applications pratiques. Des chercheurs du CNRS et Télécom ParisTech viennent ainsi de publier dans la revue *Nature Partner Journal Quantum Information* le résultat de leurs travaux de recherche sur les applications de l'informatique quantique sur les cryptomonnaies, .

Signé par 6 experts (Mathieu Bozzio, Adeline Orieux, Luis Trigo Vidarte, Isabelle Zaquine, Iordanis Kerenidis et Eleni Diamanti), « *Experimental investigation of pratical unforgeable quantum money* » décrit les expérimentations qu'ils ont menées autour des applications pratiques des travaux théoriques de Stephen Wiesner et du théorème d'« anti-clonage ».

Ce dernier stipule qu'il est physiquement impossible de cloner un système quantique inconnu, autrement dit de générer deux copies identiques d'un système en partant d'une simple copie.

Wiesner avait ainsi montré en 1983 que cette caractéristique pouvait être utilisée pour protéger une information chiffrée de toute contrefaçon : la propriété quantique de non-clonage empêche « mécaniquement » un tiers malveillant de récupérer des informations du système quantique sans le perturber.

Protéger une transaction financière consiste fondamentalement à garder une trace de chaque transaction, tout en s'assurant que l'information transmise ne soit ni pervertie ni dupliquée.

C'est par exemple le rôle typique du fameux registre qui sert de fondation aux blockchains (elles-mêmes au cœur des cryptomonnaies actuelles).

Les cryptomonnaies actuelles s'appuient sur les blockchains et sur des hypothèses « computationnelles » (autrement dit des calculs algorithmiques) pour protéger l'information.

Selon une contribution officielle (schéma à l'appui), les chercheurs du CNRS et de Télécom ParisTech ont développé un protocole et une monnaie quantique qui tirent profit des propriétés anti-clonage de la physique quantique pour protéger « mécaniquement » les transactions sans faire appel à des calculs algorithmiques qui peuvent potentiellement être pervertis.

Leur objectif à terme est de mettre en œuvre des mémoires quantiques pour expérimenter l'idée de cartes bancaires quantiques…

(Crédit photo : Shutterstock-archive : Welcomia)