GPG fingerprint for stie@itk.swiss:
1AB4 D367 AA1E 40BA D853 C029 253A

Blockchain :

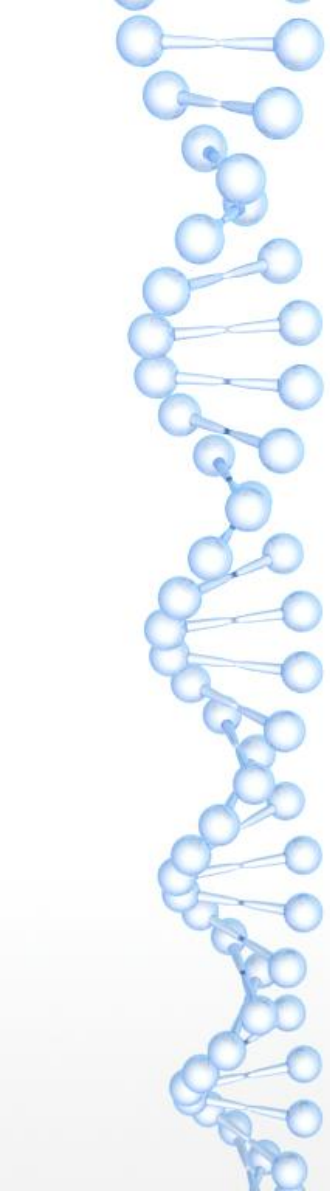
Risques et opportunités à l'heure du quantum computing (informatique quantique)

Stiepan A. Kovac, conférencier au FOREP 2019,
Événement SAQ à "La Marive", Yverdon, Suisse

FORUM Excellence Performance

Introduction

- Les technologies blockchain, dont le plus célèbre représentant à ce jour est la blockchain liée à la cryptomonnaie Bitcoin, elle-même basée sur des algorithmes de hachage et signatures numériques (techniques cryptographiques), ont toutes un point commun : elles sont aussi sécurisées que leurs briques de base, cryptographiques, le sont. "Es ist nur eine Frage der Zeit."
- La cryptographie est devant une révolution, celle de l'informatique quantique, qui va casser l'essentiel des chiffrements actuellement utilisés partout (banques, web, …), dans la prochaine décennie, d'après ceux qui

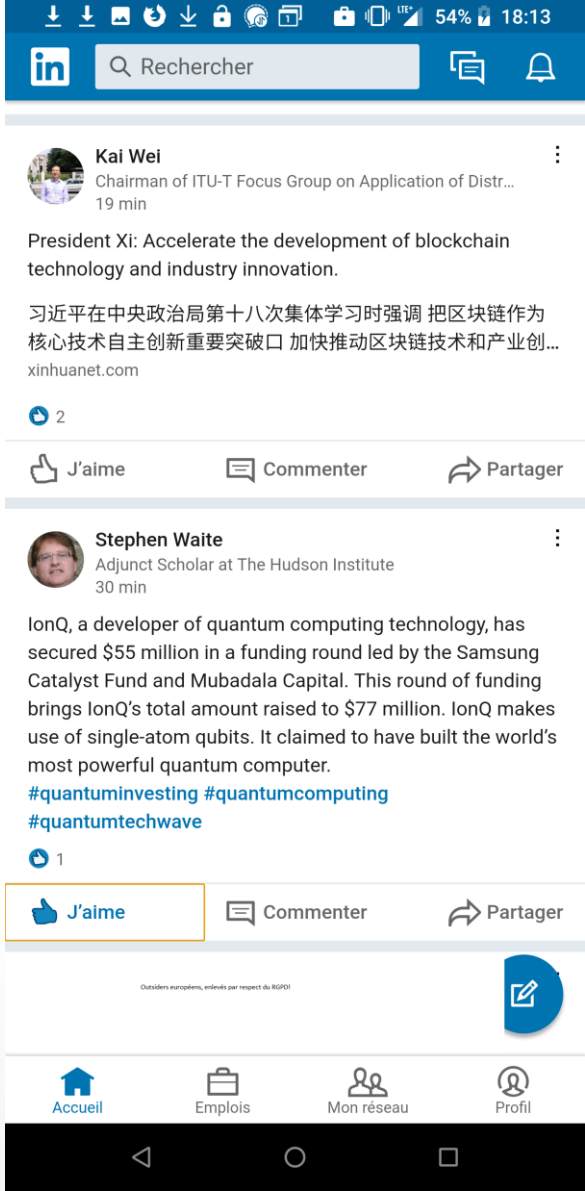


Le cas d'école : Bitcoin

- Bitcoin, à l'instar de Windows pour les systèmes d'exploitation PC, a la particularité d'être la plus connue et utilisée des cryptomonnaies. Ceci l'expose à toutes sortes d'attaques et il s'en sort assez bien jusqu'ici, malgré des fiascos tout aussi isolés que retentissants.
- Hormis les attaques quantiques, les systèmes blockchain basés sur la *proof-of-work*, telle la blockchain liée à la cryptomonnaie Bitcoin, sont vulnérables aux dites « attaques à 51 % » : si la majorité des nœuds de minage (effectuant les calculs cryptographiques) était piratée, alors tout le système tomberait, dans la mesure où le pirate en prendrait les rênes.

À la recherche du meilleur « petit bouton rouge » (dixit *kill switch*)

- La capture d'écran ci-contre illustre parfaitement le volet technologique de la guerre commerciale actuelle :
- En haut, une citation de Xi Jinping, qui veut accélérer le développement de l'industrie du blockchain en Chine
- En bas, La Start-up quantum IT U.S.

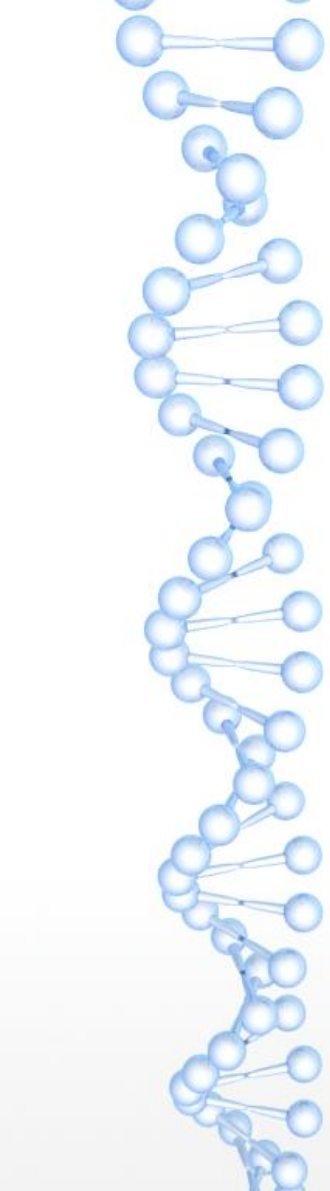


Le cas d'école : Bitcoin (suite)

- Attaques à 51 % à part, la menace quantique est tangible pour Bitcoin (et tous ses dérivés) en raison d'une décision de design lourde de conséquences, aux motivations plus politiques que techniques : Bitcoin utilise RIPEMD-160 (UE) en plus de SHA-2 256 (NSA), or comme le nom du premier l'indique, il n'utilise que 160 bits, or, on sait que seuls les variantes à 256 ou + bits devraient y résister*.
- →avec l'IT quantique, le serpent se mord la queue ; « diabolicum perseverare ».
- En outre, se baser sur SHA-2 est discutable, alors que SHA-3 existe et a été élu, publiquement, devant lever

Le « meilleur » élève : TheQRL

- En réponse aux menaces planant sur les blockchains basées sur de la cryptographie actuelle, une initiative se démarque des autres, TheQRL.org, en utilisant les signatures XMSS qui sont désormais standardisées par l'IETF et ont pour but d'être résistantes à l'ordinateur quantique (et qui sont par ailleurs recommandées par X.1197amd1 dans le contexte de l'IPTV).
- Les guillemets du titre tomberaient si TheQRL avait résolu la quadrature du cercle au niveau blockchain, à savoir résister aux attaques à la majorité (comme celles à 51 % de Bitcoin).



Opportunités du quantum computing

- Assez parlé de risques, venons-en aux opportunités !
- Le quantum computing, de par la capacité massive de calcul parallèle qu'il fournit, marquera le début d'une nouvelle ère en matière de recherche médicale, en même temps qu'il sonnera le glas de la crypto (-graphie et monnaie) grand-public actuelle.
- Au niveau cryptographie, la montée en puissance de calcul du quantum computing exigera l'excellence comme minimum, contrairement au focus encore actuel sur la performance uniquement, au détriment de la sécurité notamment.

Opportunités du quantum computing (suite)

- Les points précédents nous amènent à penser dès aujourd'hui des systèmes blockchain excellents d'un point de vue sécuritaire et performants, ce qui ne va pas de soi, les deux semblant à priori contradictoires, mais est nécessaire à la survie des blockchains.
- Au niveau de la cryptographie symétrique, utilisée pour chiffrer de la donnée sur une blockchain – une façon de respecter le RGPD – une opportunité que nous avons identifié se trouve dans l'amélioration de l'existant (AES) pour qu'il résiste à l'ordinateur quantique sans impact majeur sur la performance : cf. https://eprint.iacr.org/2019/553 (ibid) .

Des questions ?

- Contact : Stiepan Aurélien Kovac, expert en cryptographie auprès du WG2 de l'ISO SC27 et de l'ISO TC68 (ce dernier pour le compte de la SKSF), ainsi qu'auprès de la chambre d'experts de l'UTS. Membre du comité de révision SAC 2020 (ACM/SIGAPP).
- E-mail : stie at itk point swiss (empreinte GPG ci-après)
- +41 26 466 10 84 / +41 22 734 59 96 (redir. sur mob.)
- 45WU555A (sur Threema)

Cyber-Security Development

GPG fingerprint for stie@itk.swiss:
1AB4 D367 AA1E 40BA D853 C029 253A

Merci pour votre attention !