Quantum & blockchain

Best friendmies !

Introduction

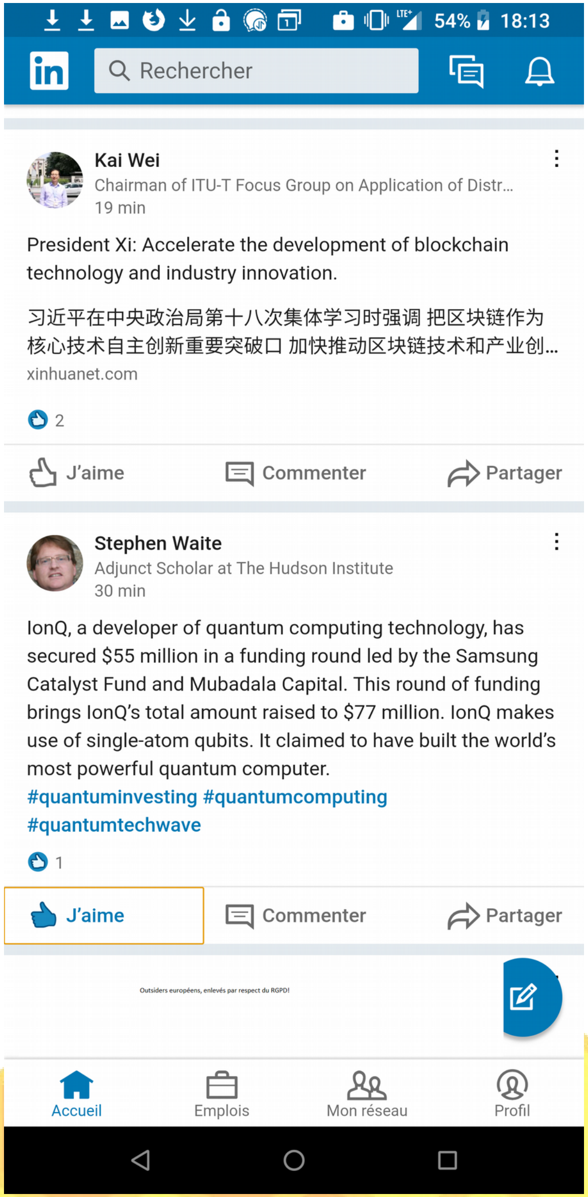
- Blockchain technologies, of which the most famous representative is the Bitcoin crypto currency, all have a point in common (hacker thinking : single point of failure) : cryptography.
- Blockchains are thus as secure as their crypto building blocks are ; *es ist nur eine Frage der Zeit*. Note that it applies to other applications too, wherever cryptography is used (PKI, etc.).

The most common example

- Bitcoin, like Windows for PCs, is known to be the most famous cryptocurrency. That exposes it to attacks and it fares pretty well so far, amid resounding isolated failures and ripoffs.
- An important point of failure besides crypto in bitcoin is its consensus mechanism, called « proof-of-work » : it is exposed to majority attacks, meaning whoever has 51 % of the « mining power » controls the ecosystem.

In search for the best *kill switch*

- This screen captures illustrates the technological side of the raging trade war : btc vs quantum
- Above, a quote of the head of state of the PRC, « accelerate blockchain development »
- Below, The US quantum start-up



54 % 18:13

Rechercher

Kai Wei
Chairman of ITU-T Focus Group on Application of Distr...
19 min

President Xi: Accelerate the development of blockchain technology and industry innovation.

习近平在中央政治局第十八次集体学习时强调 把区块链作为核心技术自主创新重要突破口 加快推动区块链技术和产业创...
xinhuanet.com

2

J'aime Commenter Partager

Stephen Waite
Adjunct Scholar at The Hudson Institute
30 min

IonQ, a developer of quantum computing technology, has secured $55 million in a funding round led by the Samsung Catalyst Fund and Mubadala Capital. This round of funding brings IonQ's total amount raised to $77 million. IonQ makes use of single-atom qubits. It claimed to have built the world's most powerful quantum computer. #quantuminvesting #quantumcomputing #quantumtechwave

1

J'aime Commenter Partager

Outsiders européens, enlevés par respect du RGPD!

Who is David and who is Goliath ?

- Besides 51 % attacks, the quantum threat to Bitcoin (and its forks) is real, due to a design decision with more political than technical background : Bitcoin uses RIPEMD-160 (EU) in addition to SHA2 256 (NSA). Nakamoto anyone ?
- As the first one’s name implies, it uses only 160 bits, and we know that only 256+ bit hashes and symmetric encryption will resist quantum attacks.
- Furthermore, like Eth it uses ECC (Shor breaks it)

What could’ve/be(en) done better ?

- Nowadays, to base on SHA-2 whereas SHA-3 exists and has been selected out of a public competition is probably not the wisest choice.
- However, SHA-3 has its limits too (block size).
- There is an example standing out : TheQRL.
- Unfortunately, it is not majority attack-proof.
- You/we/they can do better !

Opportunities of quantum

- Quantum computing is poised to open a wide range of new medical calculation possibilities, which further reinforces the case for strong data protection regulation and therefore, encryption.
- Quantum key distribution can be used to solve some of the issues of key management for high-value cryptocurrency portfolios / « wallets ».

Opportunities of quantum (2)

- Wrt symmetric crypto, used to encrypt data on blockchains – a way to fullfill GDPR if strong enough crypto is used – an opportunity lies in improving the exisiting AES, making it quantum resistant without major perf. impact : cf. https://eprint.iacr.org/2019/553 (ibid).
- The former can be combined with QKD, as the ground work done in that direction at the ITU-T has shown. In parallel, eAES started an ISO SP

Any questions ?

- Contact : Stiepan Aurélien Kovac, crypto expert at ISO SC27’s WG2 and ISO’s TC68 (for the SKSF.ch). SAC 2020 reviewer (ACM/SIGAPP).
- E-mail : stie at itk point swiss (GPG fingerprint below)
- +41 26 466 10 84 / +41 22 734 59 96 (redir. on mobile)
- 45WU555A (on Threema)

Cyber-Security Development

itk

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

Thanks for your attention !