

*Renaud Lifchitz est un expert français reconnu en sécurité informatique ayant une longue expérience d'auditeur et de formateur, principalement dans les secteurs bancaire et télécom. Il s'intéresse tout particulièrement au développement sécurisé, aux protocoles de communication sans fil et à la cryptographie. Il a été intervenant dans de nombreuses conférences internationales et a formé directement plus de 1800 personnes. Ses travaux de sécurité les plus significatifs portent sur les thèmes : cartes bancaires sans contact, géolocalisation GSM, blockchain, signatures RSA, ZigBee, Sigfox, LoRaWAN, Vigik et calcul quantique.*

### **Expériences blockchain :**

- Utilisateur de bitcoin depuis 2010
- Printemps 2011 : auteur de la première présentation publique en France sur le bitcoin
- Conception de la preuve de travail de DataCoin et PrimeCoin (fonction "EulerLagrangeLifchitzPrimalityTest") qui a battu plusieurs dizaines de record du monde en théorie des nombres
- 2013 : Conception d'un dispositif de minage de Bitcoin sur FPGA, profitable pendant 2 ans
- 2013-2020 : Développement autour de la blockchain et de smart contracts
- 2017-2020 : Conseil blockchain et auditeur cybersécurité pour une vingtaine de projets blockchain, plusieurs dizaines d'interviews medias
- 2018 : Contributeur au rapport parlementaire de l'OPECTST (Sénat) sur la blockchain : <https://www.senat.fr/notice-rapport/2017/r17-584-notice.html>

### **Mini-résumé de l'intervention : "Blockchain et cybersécurité"**

Les blockchains introduisent de nouveaux concepts et de nouvelles opportunités, mais aussi des spécificités dans l'approche de la sécurité. Quelles sont ces nouveaux risques ? Comment les traiter et les intégrer dans le choix d'une architecture blockchain, dans le choix d'une technologie, dans la conception d'un projet et dans son implémentation pratique ?