CYCLE / HISTOIRE DE L'INFORMATIQUE ET DU NUMÉRIQUE

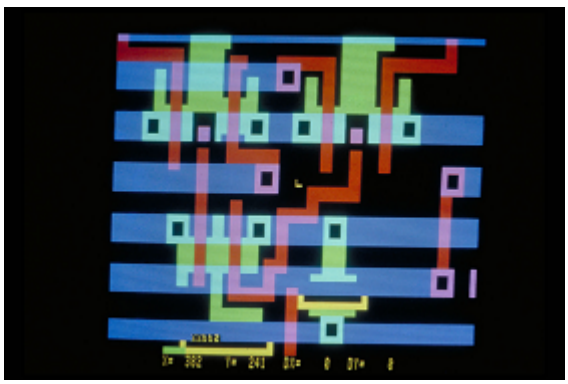
Histoire de la monnaie électronique et des blockchains avant le bitcoin

Avec Jean-Jacques Quisquater a été à l'origine, au niveau mondial, de nouvelles cartes à puce incluant toute la cryptographie forte d'alors (DES, RSA, ...), toujours utilisées aujourd'hui. Il a également travaillé sur le watermarking et les blockchains.

Bitcoin et les blockchains résultent d'une convergence assez unique de contexte (la crise financière de 2008) et de résultats, expériences et recherches diverses qui commencent vers 1980. Qui en sont les acteurs principaux ? Sans doute, Leslie Lamport pour tout ce qui concerne le consensus (élection d'un chef dans un réseau distribué), David Chaum pour ses contributions à la protection de la vie privée et à l'idée de monnaie électronique (comment éviter de payer deux fois avec le même jeton : sa solution était géniale mais peu compréhensible).
Ce fut sans doute la réalisation effective de réseaux pair-à-pair (kazaa, napster, eMule, ...), oui, soyons clair, des pirates, qui permit à chacun de comprendre la puissance des réseaux P2P. La cryptographie originale imaginée par Merkle permit enfin à Stuart Haber et Scott Stornetta de réaliser pratiquement la première blockchain en utilisant le New York Times (version papier). Ce fut le projet belge TIMESEC (1996) qui implémenta en pratique la première version des blockchains sur internet.
Et l'histoire complète est bien plus étonnante !

Jean-Jacques Quisquater a travaillé chez Philips Research entre 1970 et 1991 : ses sujets de recherches furent l'optimisation des circuits d'ordinateurs, puis tout le champ de la cryptographie. Il fut à l'origine, au niveau mondial, de nouvelles cartes à puce incluant toute la cryptographie forte d'alors (DES, RSA, ...), toujours utilisées aujourd'hui. Il a eu aussi l'occasion de travailler sur le watermarking et les blockchains (qui ne portait pas encore ce nom). En 1991, il est invité à l'Université de Louvain où il perfectionne ses recherches antérieures. Il fonde alors un groupe de recherches combinant informatique, mathématiques, circuits logiques, télécommunications et preuves de programme, modèle de collaboration qui diffusa dans le monde. Il est membre à vie de l'IEEE, académicien titulaire à l'Académie royale de Belgique, et membre d'honneur de l'ARCSI, l'Association des réservistes du chiffre et de la sécurité de l'information.

+ Tout sur les séminaires Histoire de l'informatique et du numérique



16 mai 2019
14h30 - 17h

Paris Saint-Martin/Conté

amphithéâtre Abbé-Grégoire

Envoyer un courriel ✉

▶ Entrée sur inscription gratuite : isabelle.astic@lecnam.net

▶ La séance sera également retransmise en direct sur internet.
Si vous êtes intéressé.e, le lien vous sera communiqué sur simple demande, au plus tard 2 jours avant la séance.