Les crypto-monnaies privées

ECTS : 2

Volume horaire : 18

Description du contenu de l'enseignement :

La première partie du cours qualifie le projet visant à créer un système d'espèces électroniques, étudie les problèmes posés par son opérationnalisation et les solutions envisagées jusqu'à Bitcoin. La deuxième partie du cours explore les motivations politiques derrière la conception de systèmes d'espèces électroniques.

Compétence à acquérir :

Le cours explore la genèse et le développement des cryptomonnaies privées. Les étudiant.e.s devront être capables de :

- Connaître les défis liés à l'élaboration d'espèces électroniques (ex: la gestion de la double-dépense).
- Présenter les procédés cryptographiques permettant de chiffrer les paiements électroniques (ex: les fonctions aveugles).
- Expliquer les conditions d'émergence de Bitcoin et de ses alternatives (ex: Ripple, Ethereum, ZCash).
- Rationaliser la conception de systèmes d'espèces électroniques.

Mode de contrôle des connaissances :

Examen sur table (60%) et Quizz (40%).

Bibliographie, lectures recommandées :

Brunton, F. 2019. Digital Cash : The Unknown History of the Anarchists, Utopians, and Technologists who Created Cryptocurrency, Princeton University Press.

Chaum, D. 1983. “Blind Signatures for Untraceable Payments,” Advances in Cryptology, Proc. Crypto’82, D. Chaum, R.L. Rivest, and A.T. Sherman, Eds., Plenum Press, New York, pp. 199-203.

Chaum, D. 1985. “Security Without Identification: Transaction Systems to Make Big Brother Obsolete,” Communications of the ACM, 28, pp. 1030-1044.

Nakamoto, S. 2008. “Bitcoin: A Peer-to-Peer Electronic Cash System,” https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html.

Turner, F. 2006. From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism, The University of Chicago Press.