Introduction aux blockchains

Introduction aux blockchains	**ECTS**		2	**SEMESTRE**	S8
8KUETN12	CM	TD	TP	EI	Travail personnel
	7h	14h	0h	0h	14h

Langues d'enseignement	Français par défaut, anglais sur demande
Responsable(s)	Xavier Goaoc blocked URL
Mots clefs	blockchain, algorithmique distribuée, cryptographie
Prérequis	cours d'informatique de première année, goût pour les maths-info

Objectif pédagogique

A l'issue du module, les étudiants seront en mesure de comprendre les fondements scientifiques des chaînes de blocs et certains de leurs enjeux applicatifs.

Organisation et contenus

Les "chaine de blocs" ("blockchain" en anglais) sont des systèmes numériques qui visent à construire de la confiance entre des acteurs qui ne se connaissent pas. Elles ambitionnent de se substituer à diverses structures de nos sociétés humaines : certification de chaine logistique, enregistrement de contrat, tenue de cadastre, système monétaire, ...

Techniquement, une chaine de blocs est un système d'enregistrement d'information, c'est-à-dire un registre, qui combine deux propriétés. D'une part, ce registre est **décentralisé** au sens où il est entretenu et mis à jour conjointement par un ensemble d'acteurs indépendants les uns des autres. D'autre part, ce registre est **infal sifiable** au sens où il est facile pour chaque acteur de déterminer si une copie donnée du registre a été altérée.

La conception d'une chaine de blocs met en jeu de la **cryptographie** et du **calcul distribué**. Différents choix techniques (algorithmes, fonctions mathématiques, ...) conduisent à différents types de chaines de blocs et, in fine, donnent différents sens aux mots ``acteurs indépendants'' et ``infalsifiable''. Appréhender le sens de ces adjectifs dans une chaine de bloc donnée demande d'examiner ses principes de fonctionnement. Ce cours a pour objectif de vous donner les bases scientifiques pour mener une telle analyse.

Le cours commence par trois séances de cryptographie dédiées au **hachage** et à la **signature**. Ensuite, vient une séance posant le cadre du **calcul distribué** et plus précisément les problèmes de l'**élection** et du **consensus**. Avec ces notions à notre disposition, on peut alors procéder à une **étude de cas** sur le *bitcoin*, plus précisément son élection par **preuve de travail**, son **consensus probabiliste**, sa **capacité sérieusement limitée** et son **empreinte écologique catastrophique**. Suivent deux autres séances de calcul distribué dévolues respectivement aux **barrières théoriques** limitant l'horizon des possibles en calcul distribué et à quelques **algorithmes de consensus**.

La version courante du polycopié du cours est disponible à https://members.loria.fr/XGoaoc/

Compétences

Niveaux	**Description et verbes opérationnels**
Connaître	• les notions de base en algorithmique distribuée et en cryptographie intervenant dans les chaines de blocs, • les principaux modèles de chaînes de blocs, • les barrières théoriques en calcul distribué qui limitent les solutions techniques envisageables.
Comprendre	• comment une chaîne de blocs concilie les objectifs a priori contradictoires de sécurité et de décentralisation, • comment fonctionne le système bitcoin et pourquoi son coût énergétique est aussi déraisonnable.
Appliquer	
Analyser	Le coût de fonctionnement et les garanties (décentralisation et sécurité) d'une chaîne de bloc.
Synthétiser	
Évaluer	

Contributions aux Objectifs de Développement Durable des Nations Unies

Modalités de contrôle des connaissances et compétences

Contrôle Continu	☑	Examen écrit	☐	Oral / Soutenance	☐	Rapport / Projet	☑