Module : Blockchain				Code	
				ING-4-SSIR-S7-P1	
Période	**Semestre 1**	*Volume horaire*	**42 heurs**	*ECTS*	**3**

Responsable	**Rim Farhat**	*email*	Rim.farhat@tek-up.de
Equipe pédagogique			

1. Objectifs de Module *(Savoirs, aptitudes et compétences)*

Ce module porte sur La technologie Blockchain

Acquis d'apprentissage :

A la fin de cet enseignement, l'élève sera capable de :

- Maîtriser, les bases du fonctionnement de la technologie blockchain (**C1.2**)
- Identifier les besoins de l'utilisation de la Blockchain dans plusieurs domaines (**C1.2**)
- Concevoir et Appliquer des solutions Blockchain pour plusieurs cas d'études (**C1.1**)
- Simuler et tester une Blockchain (**C1.3**)
- Concevoir des contrats intelligents (**C1.1**)
- Communiquer et déployer les contrats intelligents (**C3.3**)
- Consolider la compréhension des concepts clés des vulnérabilités des contrats intelligents (**C3.3**)

Compétences
C1.2 Maîtriser, les bases du fonctionnement de la technologie blockchain Identifier les besoins de l'utilisation de la Blockchain dans plusieurs domaines
C1.3 Simuler et tester une Blockchain
C3.3 Communiquer et déployer les contrats intelligents
C1.1 Concevoir et Appliquer des solutions Blockchain pour plusieurs cas d'études Concevoir des contrats intelligents

2. Pré-requis*(autres UE et compétences indispensables pour suivre l'UE concernée)*

- Quelques notions cryptographiques
- Connaissances basiques de la programmation.

3. Répartition d'Horaire de Module

Intitulé de l'élément d'enseignement	*Total*	*Cours*	*TD*	*Atelier*	*Mini Projet*
Module : Blockchain	42	19.5	0	18	4.5

4. Méthodes pédagogiques et moyens spécifiques au Module

(pédagogie d'enseignement, ouvrages de références, outils matériels et logiciels)

- Supports de Cours
- Projecteur et Tableau
- Travaux pratiques
- Outils de simulation.

Bibliographie

Titre	Auteur(s)	Edition
Bitcoin: A Peer-to-Peer Electronic Cash System	Satoshi Nakamoto	2008
Blockchain Technology Implementation in the Energy Sector: Comprehensive Literature Review and Mapping	Nourcherif Gharbi Nadhira Khezami	2022
Course Guide Blockchain Developer 2019	IBM MEA Skills Academy Aldred Benedict Max Blanck Gerhard Dinhof	2019
Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform	By Vitalik Buterin	2014
Build your own decentralized applications with Ethereum and smart contracts	Xun (Brian) Wu Zhihong Zou	2019
Getting Started with Ethereum: A Step-by-Step Guide to Becoming a Blockchain Developer	Davi Pedro Bauer	2022

5. Contenu *(Descriptifs et plans des cours / Déroulement / Détail de l'évaluation de l'activité pratique)*	Durée allouée	
Module 1 : Blockchain		
Séance 1 • Naissance de Blockchain • Introduction générale à la Blockchain Bitcoin. • Présentation des Fonctions de Hashage • Description des Transactions dans BitCoin • TP : o Simulation des Fonctions de Hashage o Simulation d'un réseau Blockchain Bitcoin	Cours + Atelier	3H
Séance 2 • Principe de la plus longue chaine • Double dépense • Explication des UTXO • TP : o Investigation du principe de la plus longue chaine et de la double dépense. o Création des UTXO	Cours + Atelier	3H

Séance 3 • Protection contre les fraudes • Introduction à la cryptographie • Présentation des différents types de chiffrement • Signature électronique • Présentation complète d'un nœud de la Blockchain Bitcoin • Différents Types de portefeuilles • TP : o Téléchargement, installation et test de quelques portefeuilles desktop et mobile. o Génération des clés privés et publiques o Exploration en lignes des Blocks de la blockchain Bitcoin	Cours + Atelier	3H
Séance 4 • Différents types de la blockchain • Etude comparative entre la Blockchain privée et publique • Présentation des consensus • Etude comparative entre quelques consensus • Cas d'étude de l'utilisation d'une Blockchain • Mini Projet1 : test d'un exemple des dapps • Mini Projet2 : Analyse de contrats vulnérables célèbres (comme le cas de DAO, Parrity Wallet, etc.) et identification des erreurs critiques.	Cours + Atelier	3H
Séance 5 • Introduction et histoire de Ethereum • Présentation de l'EVM (machine virtuelle de Ethereum) • Présentation d'un compte Ethereum • Smart Contract dans Ethereum • Comparaison entre EOA (external owned account) et CA (contract account) • Domaines d'pplication de Ethereum • Comparaison entre la Blockchain Ethereum et la Blockchain Bitcoin • Processus des transactions dans Ethereum	Cours	3H
Séance 6 • TP : o Exploration des Blocks dans Ethereum o Simulation d'une Blockchain Ethereum (Création de nœud, Génération des clés privés et publiques, Création de comptes, Minage, Transaction de transfert de valeurs)	Atelier	3H
Séance 7 • TP : o Développement, test et déploiement de quelques contrats intelligents (Solidity, Remix, Truffle, Ganache, …) o Création de Token et utilisation de MetaMask	Atelier	3H
Séance 8 • Validation mini-projet 1	Atelier	3H
Séance 9	Cours	3H

• Importance de la sécurité dans le développement de smart contracts. • Introduction à l'Audit des Contrats Intelligents • Expliquer les méthodologies pour l'audit manuel et automatisé des contrats intelligents. • Principales vulnérabilités : reentrancy, overflow/underflow, gas limit/gas price, etc.		

Séance 10
• Validation mini-projet 2
• Analyse de Cas Réels : DAO et Parity Wallet
  ○ Identification des Vulnérabilités
  ○ Impact et Conséquences
  ○ Leçons Apprises et Bonnes Pratiques
	Cours + Atelier	3H

Séance 11 • Discussion sur l'importance de l'audit de sécurité et des bonnes pratiques de développement sécurisé. • Introduction au outil d'analyse statique MythX: • TP : Analyse Statique des Contrats Intelligents avec MythX et Interprétation des Résultats	Cours + Atelier	3H
Séance 12 • Introduction à l'outil d'analyse statique Securify : • TP : Analyse Statique des Contrats Intelligents avec Securify et Interprétation des Résultats	Cours + Atelier	3H
Séance 13 • TP : Exercice de Défense ○ Modifier un contrat intelligent pour corriger les vulnérabilités identifiées.	Atelier	3H

Séance 14
• Quiz pour évaluer la compréhension des participants sur les vulnérabilités des contrats intelligents et les mesures de sécurité.
• Exercice de Réflexion : Défis et Bonnes Pratiques
  ○ Identification des défis spécifiques rencontrés lors de l'audit et de la sécurisation des contrats intelligents.
  ○ Discussion sur les bonnes pratiques recommandées pour prévenir ces défis.
	Cours + Atelier	3H

6. Mode d'évaluation de Module*(nombre, types et pondération des contrôles)*

Eléments d'enseignement	Coeff	DS	EX	TP	PR
Blockchain	2		50%	30%	20%

Pour valider le module, les étudiants passeront un examen dont le coefficient est de 50%, un projet dont le coefficient est de 20% et un TP dont le coefficient est de 30%.

La durée de tous les examens (Examen, DS…) est de 1h30.

Quand à l'examen, il est planifié après l'écoulement des 14 semaines et portera sur toutes les thématiques enseignées tout au long des 42 heures.

Concernant le TP, il est planifié une semaine avant l'examen et testera les connaissances acquises tout au long du module.

Le module est validé si l'étudiant obtient une moyenne supérieure ou égal à 10 sur 20.