CÉGEP SHAWINIGAN
Formation continue et services aux entreprises

LA SÉCURITÉ DE LA BLOCKCHAIN

PLAN DE COURS

Certification collégiale

9 HEURES

DESCRIPTIF

Cette formation a été développée pour répondre à un besoin de formation dans une technologie émergente: la blockchain. Cette Certification collégiale s'adresse principalement aux conseillers en sécurité étant intéressés de développer leurs compétences en sécurité blockchain ainsi qu'aux programmeurs pour améliorer la sécurité de leur code. Ce cours s'adresse aussi aux gestionnaires qui souhaiteront comprendre la sécurité blockchain en général afin de mieux encadrer toute la gestion des opérations tout en considérant les enjeux de sécurité.

De plus, certaines personnes du domaine juridique telles que des avocats et notaires gagneront à mieux comprendre la sécurité de la blockchain afin de mieux apprécier l'encadrement de ces éléments de réglementation faisant partie du domaine de la sécurité de la blockchain.

Ce cours a comme objectif de permettre à l'étudiant de comprendre que plusieurs éléments de sécurité sont nécessaires afin de bien encadrer méthodiquement la sécurité de la blockchain. Cette formation tient aussi compte des divers types de blockchains et de leur environnement, existant à ce jour.

Cette formation lui permettra de comprendre les différents volets de sécurité à considérer afin d'éliminer ou de minimiser les plus grandes vulnérabilités de sécurité pouvant être désastreuses à la blockchain.

Ce cours s'adresse principalement à trois auditoires :

- Les gestionnaires qui seront chargés soit d'encadrer les opérations ou de prendre des décisions stratégiques sur l'utilisation de la technologie blockchain,
- Les conseillers en sécurité qui seront chargés d'analyser, d'évaluer ou de conseiller les éléments de sécurité à considérer et prévoir selon le type et l'environnement d'une blockchain,
- Les programmeurs blockchain afin de connaître les bonnes pratiques sécuritaires en matière de programmation et saisir les risques à du code déficient.

* Blockchain est un terme anglais utilisé en raison de sa compréhension et de son emploi très répandus dans le domaine des technologies de l'information. L'équivalent français de blockchain est chaîne de blocs.

COMPÉTENCES

Pour atteindre l'objectif visé par ce cours, soit d'approfondir leur connaissance dans la sécurité de la blockchain et d'acquérir les compétences nécessaires à bien conseiller et orienter les divers aspects entourant sa sécurité, l'étudiant devra développer les éléments de compétence suivants :

- ◊ Comprendre les fondements de la sécurité qui s'applique aux éléments composants la blockchain ainsi que les principales fonctions cryptographiques utilisées,
- ◊ saisir l'importance des consensus de la blockchain afin d'en réguler des transactions sécuritaires,
- ◊ distinguer les divers mécanismes cryptographiques sécuritaires de transactions et de manipulation d'information,
- ◊ connaître les différents types d'audit de sécurité s'appliquant aux contrats intelligents et savoir considérer la sécurité nécessaire à appliquer aux informations ou aux actifs informationnels transigés,
- ◊ comprendre les notions de risque et reconnaître les risques de sécurité inhérents aux types de blockchains,
- ◊ reconnaître les diverses propriétés des types de blockchains afin de mieux considérer la criticité des éléments de sécurité à appliquer,
- ◊ reconnaître certaines réglementations entourant la blockchain et ces dérivés, dont les cryptomonnaies et autres,
- ◊ connaître les principales vulnérabilités et types d'attaques utilisées contre l'écosystème de la blockchain.

CONTENUS ESSENTIELS

Vue d'ensemble de la progression des apprentissages et des contenus essentiels :

1. LES FONDEMENTS

Objectif(s) : comprendre les fondements de la sécurité ainsi que ceux de la blockchain.

- Les trois fondements de base de la sécurité : disponibilité, intégrité et confidentialité,
- la cryptographique, la base nécessaire qui garantit la sécurité de la blockchain,
- les fonctions de hachages,
- le chiffrement symétrique et asymétrique,
- le principe des clés publiques ,
- les algorithmes RSA et ECC ,
- les propriétés de sécurité particulières et requises à la blockchain pour les blocs, les chaînes et les réseaux,
- revue des bénéfices de sécurité en rapport aux propriétés des éléments de la blockchain,
- les types de gestion de clés privées,
- la quantique et la blockchain.

2. LE CONSENSUS

Objectif(s) : saisir les nuances de sécurité sur des consensus différents. Comprendre que chaque type de consensus nécessite d'être sécurisé différemment.

- Présentation et explication du problème des « Généraux Byzantins » et la tolérance aux fautes,
- les éléments de sécurité à considérer selon le type de consensus utilisé.

3. SOLUTIONS CRYPTOGRAPHIQUES AVANCÉES

Objectif(s) : savoir qu'il existe divers mécanismes cryptographiques pour effectuer des transactions, des échanges ou des transferts d'information sécuritaires entre les parties.

- présentation des différents types de signatures d'autorisation ainsi que leurs possibilités permettant des échanges demandant de la confidentialité ou plusieurs autorisations,
- les possibilités d'anonymiser sécuritairement les émetteurs et/ou les destinataires ,
- les méthodes de confidentialité des transactionnelles,
- la mise à profit des concepts mathématiques.

4. SÉCURITÉ DES CONTRATS INTELLIGENTS

Objectif(s) : connaître les principaux risques de sécurité avec les propriétés inhérentes aux contrats intelligents. Savoir qu'il existe différents types d'audit, selon les objectifs à atteindre, pour mieux évaluer et sécuriser le code des contrats intelligents.

- La notion « Turing Complet »,
- les types de contrats intelligents et leurs propriétés,
- les propriétés des contrats intelligents à considérer comme risque,
- présentation des différents types d'audit ainsi que leurs bénéfices,
- les bénéfices des audits.

5. ÉVALUATION DES RISQUES

Objectif(s) : comprendre les notions de risques en sécurité et être en mesure de reconnaître certains risques inhérents aux composants de la Blockchain. Savoir qu'il peut aussi y avoir diverses réglementations juridiques à respecter selon la vocation de la Blockchain et les types de données transigées.

- La notion de probabilité et d'impact dans l'évaluation d'un risque,
- le risque « Zéro » n'existe pas,
- survol des risques associés à la décentralisation, au grand livre distribué, à l'infrastructure et aux contrats intelligents ainsi qu'à toutes les propriétés de ces éléments.

6. SÉCURITÉ DE BASE DES BLOCKCHAINS

Objectif(s) : connaître les éléments de sécurité cruciaux à être considérés autant pour les utilisateurs, les nœuds et les réseaux

- La criticité des clés privées pour les utilisateurs,
- les vulnérabilités et les mises à jour des différents logiciels systèmes des nœuds,
- les fournisseurs de gestion d'identification et d'authentification des membres,
- les interfaces applicatives,
- la sécurité des réseaux et les protocoles de communication utilisés.

7. BLOCKCHAIN POUR LES ENTREPRISES

Objectif(s) : reconnaître les nuances de sécurité à considérer en fonction des divers types de la Blockchain pour les entreprises.

- Les différentes Blockchains au bénéfice des entreprises,
- les particularités de sécurité de chacune d'elles,
- comparaison de leurs avantages et limites en matière de sécurité.

8. IMPLÉMENTATION SÉCURISÉE DES BLOCKCHAINS

Objectif(s) : considérer les éléments de sécurité selon divers axes tels que les opérations, la gestion des données, les infrastructures et leurs actifs ainsi que la réglementation juridique pouvant y être assujettie.

- Les avantages et considérations de sécurité de la Blockchain pour les entreprises en rapport avec :
  - les opérations,
  - la gestion des contrats,
  - la distribution des produits,
  - leur monétisation,
  - la gestion des données,
  - le contrôle des accès,
  - la conservation et la suppression des actifs,
  - l'extensibilité des infrastructures,
  - les communications sécurisées,
  - la conformité juridique et réglementaire.

9. VULNÉRABILITÉS ET ATTAQUES AU NIVEAU DU RÉSEAU

Objectif(s) : connaître les vulnérabilités et les types d'attaques les plus importantes pour la gestion des réseaux et des communications.

- Introduction aux types d'attaques réseau et à leurs provenances,
- définitions et explications du fonctionnement des attaques ainsi que des contrôles de sécurité à considérer des :
  - attaque à 51%,
  - attaque par déni de service,
  - attaque par éclipse,
  - attaque par rediffusion,
  - attaque par routage,
  - attaques de Sybil.

10. VULNÉRABILITÉS ET ATTAQUES AU NIVEAU DU SYSTÈME

Objectif(s) : connaître les vulnérabilités et les types d'attaques les plus importantes pour la gestion des systèmes et leurs applications.

- Introduction aux types d'attaques système,
- les principales attaques système importantes à considérer dues à leurs vulnérabilités système ainsi que les solutions et leçons apprises à chacune d'elle.

- Revue des attaques de :
  - Bitcoin,
  - The verge Hack,
  - EOS,
  - Lisk,
  - Bitcoin Core,
  - Minage en SPV.

11. VULNÉRABILITÉS ET ATTAQUES DES CONTRATS INTELLIGENTS

Objectif(s) : connaître les vulnérabilités et les types d'attaques les plus importantes touchant directement le code de programmation utilisé dans les contrats intelligents.

- Les raisons des vulnérabilités présentes dans les contrats intelligents
- Explications et références sur les principaux types de vulnérabilités rencontrés dans la programmation du code de contrats intelligents dont :
  - la réentrée,
  - les contrôles d'accès,
  - les fonctions arithmétiques,
  - les valeurs de retours non vérifiées,
  - les dénis de service (DoS),
  - les valeurs aléatoires,
  - les situations concurrentes,
  - la dépendance à l'horodatage,
  - la taille des variables.

12. SÉCURITÉ DES ARCHITECTURES DLT ALTERNATIVESS

Objectif(s) : savoir qu'il existe d'autres types d'architectures offrant des avantages et des limitations de sécurité différentes quant aux applications des fondements de la Blockchain.

- Retour sur la définition de la technologie des grands livres distribués,
- Définition d'un Graphique Acyclique Dirigé (DAG),
- Exemples de Blockchain basés sur le DAG,
- L'application des principes de la Blockchain sur les DAG, tels que : des mécanismes de vérification des transactions, du consensus,
- Les avantages et limitations des grands livres distribués en mode DAG quant à la décentralisation, la transparence, la scalabilité, leur vitesse d'exécution,
- Les extensions possibles telles que les canaux d'état et les chaînes latérales.

INDICATIONS MÉTHODOLOGIQUES

Ce cours sera dispensé de façon à favoriser une formation la plus adéquate possible afin d'atteindre les objectifs. Il veut aussi permettre au participant d'apprendre dans un contexte favorisant la participation et l'échange. Dans ce contexte, l'enseignement sera dispensé selon les approches suivantes :

- ◊ Des cours de type magistral,
- ◊ Des présentations de matériel audiovisuel afin de faciliter la compréhension,
- ◊ Des périodes de discussion en groupe et des mises en situation sur le ou les sujets précédemment enseignés accompagnées d'explications supplémentaires s'il y a lieu,
- ◊ Des références à des articles afin d'approfondir le sujet et favoriser le lien entre la théorie enseignée et son application en industrie,

VALIDATION DES COMPÉTENCES

Afin de permettre aux enseignants de valider l'acquisition des compétences du cours et du même coup, émettre des UFC, l'étudiant aura à réussir un examen sous forme de Quiz de questions et réponses. Soit après chaque cours.

Sommairement, ce test prendra la forme suivante :

- ◊ Un Quiz par module selon le plan de cours,
- ◊ 12 Quiz en ligne de 5 à 10 questions à choix de réponses multiples,
- ◊ Les questions se présentent selon un ordre aléatoire pour chaque étudiant,
- ◊ Les Quiz auront une durée de temps déterminée et annoncée à l'avance.

CERTIFICATION COLLÉGIALE

La certification collégiale est une formation ayant pour but l'acquisition et le développement de compétences ciblées selon le domaine. Elles ont été conçues pour répondre à différents besoins de formation des entreprises ou de secteurs spécifiques.

À la fin de la formation, une Certification sera émise aux participants qui auront démontré, par la réussite d'une évaluation, que les compétences vues pendant la formation ont bien été acquises. La certification pourrait aider un participant dans l'obtention d'un emploi ou encore permettre un avancement professionnel. Les compétences reconnues pourront également être utilisées dans une démarche de reconnaissances des acquis et des compétences (RAC).