

Concepteur développeur de solutions blockchain

RNCP41719 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Code(s) NSF	326
Formacode(s)	31004, 31067, 31006, 31032
Code(s) ROME	M1805
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	27/10/2025
Date d'échéance	27/10/2028

Certificateur(s)

UNIVERSITE PARIS-SACLAY · SIRET : 13002602400054<https://www.universite-paris-saclay.fr/>

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le métier de concepteur développeur de solutions blockchain est aujourd'hui l'un des plus recherchés dans le secteur numérique. La généralisation des cas d'usage de la blockchain (finance, logistique, santé, énergie, cybersécurité, etc.) fait émerger une forte demande de ces profils. Des secteurs comme l'industrie pharmaceutique, l'agroalimentaire ou la gestion de l'énergie s'emparent progressivement de cette technologie pour répondre à des enjeux de traçabilité, de transparence ou d'automatisation. La structuration progressive du Web3 et l'intégration croissante de l'IA dans les logiques de smart contracts renforcent l'intérêt stratégique de former des développeurs blockchain. Ces évolutions requièrent des profils hybrides, capables d'intégrer également de nouvelles compétences liées à l'optimisation énergétique, à la conception éthique et à la collaboration interdisciplinaire.

Le concepteur développeur de solutions blockchain conçoit, développe, teste, sécurise et maintient des solutions informatiques basées sur la technologie blockchain, en réponse à des besoins spécifiques exprimés par des entreprises, des institutions ou des porteurs de projet. Il intervient sur des systèmes complexes nécessitant un haut niveau de traçabilité, d'automatisation, de sécurité ou de transparence, et s'appuie pour cela sur des architectures décentralisées.

Il est capable d'intervenir sur tout ou partie d'un projet blockchain : de l'analyse du besoin à la mise en production, en passant par la conception de l'architecture technique, la rédaction du cahier des charges, le codage des smart contracts (programmes auto-exécutables inscrits sur la blockchain), le développement d'interfaces d'interaction, la sécurisation de la solution et la documentation technique.

ACTIVITÉS VISÉES

Cadrage et pilotage opérationnel d'un projet blockchain :

Analyse de la pertinence technologique, réglementaire et sécuritaire d'un projet blockchain

Contribution à la gestion de projet blockchain agile et collaboration avec les parties prenantes

Conception de l'architecture technique d'une solution blockchain sécurisée et interopérable :

Définition de l'architecture d'une solution blockchain

Choix des technologies, outils et plateformes adaptés au projet blockchain

Intégration de l'interopérabilité dans les solutions blockchain

Développement des composants techniques d'une solution blockchain (smart contracts, DApps) :

Développement sécurisé de smart contracts

Conception et développement d'applications décentralisées (DApps)

Intégration, sécurisation, test et maintien d'une solution blockchain en environnement de production :
Déploiement et maintien en condition opérationnelle d'une solution blockchain
Test fonctionnel, conformité métier et robustesse de la solution
Sécurisation des composants blockchain et gestion des vulnérabilités
Contribution à l'amélioration continue des pratiques de développement et de sécurisation
Intégration des principes de durabilité et de sobriété numérique dans le développement et le déploiement de solutions blockchain :
Évaluation et prise en compte des impacts environnementaux dans les choix techniques blockchain
Optimisation de la consommation dans le développement des composants blockchain
Adoption de pratiques DevOps éco-responsables
Intégration des projets blockchain dans la démarche RSE de l'organisation
Prise en compte des référentiels et des exigences en matière de numérique responsable

COMPÉTENCES ATTESTÉES

Déterminer la pertinence du recours à une technologie blockchain à partir de l'analyse des objectifs métiers, des flux à sécuriser ou automatiser, des typologies d'usages blockchain et de la comparaison avec d'autres solutions numériques, afin de formuler une proposition technique adaptée au contexte et aux besoins identifiés.

Analyser les contraintes d'un projet blockchain, y compris les enjeux de gouvernance des données et d'identité numérique afin d'évaluer la faisabilité et les conditions de mise en œuvre d'une solution blockchain.

Caractériser et analyser les risques liés à la conformité réglementaire (RGPD, MiCA, identité numérique, eIDAS ...) et à la cybersécurité d'une solution blockchain en amont du développement, en mobilisant des référentiels, normes et pratiques sectorielles, de sorte à prévenir les vulnérabilités juridiques et techniques du projet

Assurer une veille régulière et structurée sur les évolutions technologiques (protocoles, standards, interopérabilité, cybersécurité) et réglementaires, à partir de l'exploitation de sources spécialisées, de publications scientifiques ou sectorielles et de réseaux professionnels, pour anticiper les impacts sur les projets blockchain en cours ou à venir.

Participer à la structuration et au pilotage opérationnel d'un projet blockchain en organisant les cycles de développement selon les méthodes agiles (sprints, backlog, user stories), en priorisant les tâches techniques et réglementaires (tests de smart contracts, conformité RGPD, interopérabilité, etc.), et en mobilisant les outils de planification et de suivi adaptés, afin de garantir une exécution cohérente avec les contraintes du domaine blockchain. Suivre l'avancement des développements techniques dans un environnement blockchain en actualisant les indicateurs de progression, en identifiant et en analysant les risques et écarts, et en communiquant ces éléments à l'équipe projet, afin de soutenir les arbitrages et d'assurer la stabilité des livraisons.

Collaborer avec les parties prenantes et les membres d'équipes pluridisciplinaires (développeurs, juristes, experts cybersécurité, auditeurs smart contracts, exploitants IT), dans le respect de principes d'inclusion et par l'adoption de codes de communication propres à chaque profil, tout en mobilisant des outils collaboratifs adaptés, de sorte à garantir une compréhension partagée et une coordination fluide tout au long du cycle de développement).

Produire des livrables fonctionnels et techniques (documentation d'architecture décentralisée, guides de déploiement, fiches sur les mécanismes de consensus ou d'interopérabilité), en adaptant la terminologie et les supports aux utilisateurs, y compris en situation de handicap, et en assurant un appui à la prise en main de la solution blockchain (portefeuille numérique, interface DApp), pour garantir une appropriation optimale et sécurisée.

Concevoir l'architecture technique d'une solution blockchain en définissant la structure des composants logiciels, l'organisation des flux de données et les modalités d'échange entre les acteurs du système, en s'appuyant sur des schémas d'architecture distribuée, des outils de modélisation et une analyse des besoins métiers, afin de garantir la cohérence technique, la robustesse, la scalabilité et la maintenabilité de la solution.

Intégrer les exigences de sécurité et de conformité dès la phase de conception à partir de l'identification des risques potentiels liés aux échanges décentralisés et aux données sensibles et en appliquant les principes de « security by design », les bonnes pratiques de cybersécurité et les normes réglementaires applicables (RGPD, MiCA...), dans le but de prévenir les vulnérabilités et assurer la fiabilité et la conformité de l'architecture proposée.

Sélectionner les technologies, langages, outils et environnements adaptés au projet sur la base d'une évaluation comparative des différents types de blockchain (publique, privée, permissionnée...), langages de programmation, frameworks, outils de développement et environnements d'exécution, tout en tenant compte des contraintes du projet, en vue d'optimiser la pertinence technologique, la faisabilité du développement et la pérennité de la solution à mettre en œuvre.

Implémenter et intégrer des mécanismes d'interopérabilité dans une solution blockchain en développant ou en configurant des protocoles de communication inter-chaînes et des passerelles (bridges) pour permettre l'échange

sécurisé de données ou d'actifs entre réseaux hétérogènes, en s'appuyant sur les standards de l'écosystème blockchain (IBC, Wormhole, LayerZero, etc.) et les spécifications techniques de compatibilité, afin d'assurer la fluidité des échanges et l'ouverture de la solution à d'autres systèmes distribués.

Développer des smart contracts sécurisés et conformes aux standards du secteur (ERC20, ERC721, etc.) en traduisant les règles métiers en code exécutable sur la blockchain, en appliquant les bonnes pratiques de codage (limitation des failles critiques, réentrance, gestion des erreurs), en utilisant des environnements de développement adaptés (Remix, Hardhat, Foundry...), afin d'assurer leur fiabilité, leur compatibilité avec les outils du secteur, et leur bon fonctionnement dans un environnement décentralisé.

Concevoir des actifs numériques associés à un smart contract (jetons fongibles ou non-fongibles) en utilisant les bibliothèques standardisées de l'écosystème (OpenZeppelin, etc.), en définissant les attributs techniques et les fonctions associées (émission, transfert, contrôle d'accès), de façon à permettre la création d'éléments numériques traçables, transférables et interopérables au sein d'un système blockchain.

Développer une interface utilisateur connectée à une blockchain (DApp), en utilisant des frameworks de développement web ou mobile, en intégrant des bibliothèques de connexion à des portefeuilles numériques, et en affichant de manière dynamique les données issues des smart contracts ou du ledger, pour garantir une expérience utilisateur fluide, fiable et sécurisée dans un environnement décentralisé.

Sécuriser et rendre accessibles les parcours utilisateurs d'une application blockchain en mettant en œuvre des dispositifs de sécurisation des interactions (chiffrement, signature numérique, authentification), en respectant les exigences du RGPD, et en appliquant les règles d'accessibilité notamment définies par le RGAA et les standards WCAG pour garantir l'accessibilité des interfaces aux personnes en situation de handicap, afin d'assurer une expérience utilisateur conforme, inclusive et sécurisée.

Assurer la mise en production et la continuité opérationnelle d'une solution blockchain en préparant son déploiement dans un environnement réel, en configurant les processus d'intégration et de livraison continue (CI/CD), en assurant le suivi technique post-déploiement, et en appliquant les corrections ou évolutions nécessaires, afin de garantir sa stabilité, sa disponibilité et sa capacité à évoluer selon les besoins.

Vérifier la conformité et la robustesse d'une solution blockchain en concevant et en exécutant des tests fonctionnels à partir des exigences techniques et métiers, en simulant différents scénarios d'usage pour identifier d'éventuels défauts ou anomalies, et en analysant les performances et la résilience du code dans des conditions variées, de sorte à sécuriser le déploiement de la solution et d'en garantir la stabilité dans un environnement réel.

Auditer et sécuriser les composants critiques d'une solution blockchain en conduisant des analyses de risques, des tests automatisés et des revues manuelles sur les smart contracts, les DApps et les mécanismes d'interopérabilité, pour produire ensuite des rapports de vulnérabilités et mettre en œuvre des correctifs adaptés, dans le but de renforcer la résilience de la solution face aux menaces de sécurité.

Anticiper les évolutions des pratiques de développement et de sécurisation en assurant une veille active sur les innovations technologiques en matière de blockchain, de cybersécurité, de DevOps et d'architecture logicielle, afin d'intégrer de nouveaux outils, méthodes ou dispositifs susceptibles d'améliorer les performances, la robustesse et la sécurité des solutions

Exploiter les retours d'exploitation et les contributions des utilisateurs pour améliorer une solution blockchain, en analysant les dysfonctionnements, besoins d'évolution ou leviers d'optimisation à partir des incidents techniques, des retours terrain et des usages réels, en vue de proposer des améliorations à intégrer dans les futurs cycles de développement.

Évaluer et intégrer les impacts environnementaux d'une solution blockchain en analysant la consommation énergétique, les émissions carbone, les effets de redondance des architectures distribuées et les contraintes liées au cycle de vie des données, de sorte à identifier les principaux leviers de réduction de l'empreinte écologique

Éco-concevoir les composants d'une solution blockchain en identifiant les sources principales de consommation de gas ou de ressources dans le développement des smart contracts et des DApps, en optimisant la logique algorithmique et la structure du code, et en appliquant des principes d'écoconception adaptés aux environnements décentralisés, afin de réduire leur impact environnemental sans compromettre leurs performances.

Mettre en oeuvre des pratiques DevOps éco-responsables dans le déploiement de solutions blockchain en limitant les redondances et la fréquence des livraisons, en sélectionnant des infrastructures d'hébergement ou de cloud à faible empreinte carbone, et en configurant les environnements d'exécution de manière sobre et efficiente, afin d'assurer la soutenabilité technique et environnementale des processus de déploiement en production.

Contribuer à l'intégration de la sobriété numérique dans la stratégie RSE appliquée aux projets blockchain en participant à la définition d'indicateurs environnementaux pertinents, en identifiant les leviers d'alignement entre les choix techniques et les engagements de l'organisation, et en appuyant les démarches de sensibilisation ou

d'amélioration continue, afin de renforcer la cohérence entre innovation numérique et responsabilité sociétale. Aligner les pratiques de développement blockchain sur les référentiels et normes du numérique responsable en analysant les exigences des cadres réglementaires et sectoriels (RGESN, REEN, Green IT, ISO 14001...), en identifiant les écarts de conformité et en mettant en œuvre les ajustements nécessaires, y compris dans le cadre de démarches de certification ou de labellisation, afin d'inscrire les solutions développées dans une démarche écoresponsable structurée et reconnue.

Blocs de compétences

RNCP41719BC01 — Cadrer et piloter un projet blockchain de façon opérationnelle

LISTE DE COMPÉTENCES

Déterminer la pertinence du recours à une technologie blockchain à partir de l'analyse des objectifs métiers, des flux à sécuriser ou automatiser, des typologies d'usages blockchain et de la comparaison avec d'autres solutions numériques,

Analyser les contraintes d'un projet blockchain, y compris les enjeux de gouvernance des données et d'identité numérique,

Caractériser et analyser les risques liés à la conformité réglementaire (RGPD, MiCA, identité numérique, eIDAS ...) et à la cybersécurité d'une solution blockchain en amont du développement, en mobilisant des référentiels, normes et pratiques sectorielles,

Assurer une veille régulière et structurée sur les évolutions technologiques (protocoles, standards, interopérabilité, cybersécurité) et réglementaires, à partir de l'exploitation de sources spécialisées, de publications scientifiques ou sectorielles et de réseaux professionnels,

Participer à la structuration et au pilotage opérationnel d'un projet blockchain en organisant les cycles de développement selon les méthodes agiles (sprints, backlog, user stories), en priorisant les tâches techniques et réglementaires (tests de smart contracts, conformité RGPD, interopérabilité, etc.), et en mobilisant les outils de planification et de suivi adaptés,

Suivre l'avancement des développements techniques dans un environnement blockchain en actualisant les indicateurs de progression, en identifiant et en analysant les risques et écarts, et en communiquant ces éléments à l'équipe projet,

Collaborer avec les parties prenantes et les membres d'équipes pluridisciplinaires (développeurs, juristes, experts cybersécurité, auditeurs smart contracts, exploitants IT), dans le respect de principes d'inclusion et par l'adoption de codes de communication propres à chaque profil, tout en mobilisant des outils collaboratifs adaptés,

Produire des livrables fonctionnels et techniques (documentation d'architecture décentralisée, guides de déploiement, fiches sur les mécanismes de consensus ou d'interopérabilité), en adaptant la terminologie et les supports aux utilisateurs, y compris en situation de handicap, et en assurant un appui à la prise en main de la solution blockchain (portefeuille numérique, interface DApp),

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée à partir d'un projet blockchain réel ou fictif.

Etude de cas contextualisée.

Le candidat démontre sa capacité à analyser la pertinence technologique, réglementaire et sécuritaire d'un projet blockchain, puis à contribuer efficacement à son pilotage opérationnel et à la collaboration avec les parties prenantes, dans un cadre de projet agile.

Modalités de mise en œuvre :

Épreuve écrite individuelle (3h00)

Soutenance orale de 20 min

RNCP41719BC02 — Concevoir l'architecture technique d'une solution blockchain sécurisée et interopérable

LISTE DE COMPÉTENCES

Concevoir l'architecture technique d'une solution blockchain en définissant la structure des composants logiciels, l'organisation des flux de données et les modalités d'échange entre les acteurs du système, en s'appuyant sur des schémas d'architecture distribuée, des outils de modélisation et une analyse des besoins métiers,

Intégrer les exigences de sécurité et de conformité dès la phase de conception à partir de l'identification des risques potentiels liés aux échanges décentralisés et aux données sensibles et en appliquant les principes de « security by

design », les bonnes pratiques de cybersécurité et les normes réglementaires applicables (RGPD, MiCA...), Sélectionner les technologies, langages, outils et environnements adaptés au projet sur la base d'une évaluation comparative des différents types de blockchain (publique, privée, permissionnée...), langages de programmation, frameworks, outils de développement et environnements d'exécution, tout en tenant compte des contraintes du projet, Implémenter et intégrer des mécanismes d'interopérabilité dans une solution blockchain en développant ou en configurant des protocoles de communication inter-chaînes et des passerelles (bridges) pour permettre l'échange sécurisé de données ou d'actifs entre réseaux hétérogènes, en s'appuyant sur les standards de l'écosystème blockchain (IBC, Wormhole, LayerZero, etc.) et les spécifications techniques de compatibilité,

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée à partir d'un projet blockchain réel ou fictif.

Sur la base d'un cahier des charges métier, le candidat doit concevoir l'architecture d'une solution blockchain répondant aux exigences techniques, de sécurité, d'interopérabilité et de conformité.

Modalités de mise en oeuvre :

Épreuve écrite individuelle (3h)

Soutenance orale (20 min)

RNCP41719BC03 — Développer des composants techniques d'une solution blockchain (smart contracts, DApps)

LISTE DE COMPÉTENCES

Développer des smart contracts sécurisés et conformes aux standards du secteur (ERC20, ERC721, etc.) en traduisant les règles métiers en code exécutable sur la blockchain, en appliquant les bonnes pratiques de codage (limitation des failles critiques, réentrance, gestion des erreurs), en utilisant des environnements de développement adaptés (Remix, Hardhat, Foundry...),

Concevoir des actifs numériques associés à un smart contract (jetons fongibles ou non-fongibles) en utilisant les bibliothèques standardisées de l'écosystème (OpenZeppelin, etc.), en définissant les attributs techniques et les fonctions associées (émission, transfert, contrôle d'accès),

Développer une interface utilisateur connectée à une blockchain (DApp), en utilisant des frameworks de développement web ou mobile, en intégrant des bibliothèques de connexion à des portefeuilles numériques, et en affichant de manière dynamique les données issues des smart contracts ou du ledger,

Sécuriser et rendre accessibles les parcours utilisateurs d'une application blockchain en mettant en œuvre des dispositifs de sécurisation des interactions (chiffrement, signature numérique, authentification), en respectant les exigences du RGPD, et en appliquant les règles d'accessibilité notamment définies par le RGAA et les standards WCAG pour garantir l'accessibilité des interfaces aux personnes en situation de handicap,

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée à partir d'un projet blockchain réel ou fictif.

Application technique

Le candidat réalise, à partir d'un cahier des charges simplifié, le développement d'un smart contract et d'une interface décentralisée (DApp) associée.

Modalités de mise en oeuvre :

Epreuve réalisée sur une durée de 5 heures

Rendu des livrables techniques en fin d'épreuve

RNCP41719BC04 — Intégrer, sécuriser, tester et maintenir une solution blockchain en environnement de production

LISTE DE COMPÉTENCES

Assurer la mise en production et la continuité opérationnelle d'une solution blockchain en préparant son déploiement dans un environnement réel, en configurant les processus d'intégration et de livraison continue (CI/CD), en assurant le suivi technique post-déploiement, et en appliquant les corrections ou évolutions nécessaires,

Vérifier la conformité et la robustesse d'une solution blockchain en concevant et en exécutant des tests fonctionnels à partir des exigences techniques et métiers, en simulant différents scénarios d'usage pour identifier d'éventuels défauts ou anomalies, et en analysant les performances et la résilience du code dans des conditions variées,

Auditer et sécuriser les composants critiques d'une solution blockchain en conduisant des analyses de risques, des tests automatisés et des revues manuelles sur les smart contracts, les DApps et les mécanismes d'interopérabilité, pour produire ensuite des rapports de vulnérabilités et mettre en œuvre des correctifs adaptés,

Anticiper les évolutions des pratiques de développement et de sécurisation en assurant une veille active sur les

innovations technologiques en matière de blockchain, de cybersécurité, de DevOps et d'architecture logicielle
Exploiter les retours d'exploitation et les contributions des utilisateurs pour améliorer une solution blockchain, en analysant les dysfonctionnements, besoins d'évolution ou leviers d'optimisation à partir des incidents techniques, des retours terrain et des usages réels,

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée à partir d'un projet blockchain réel ou fictif.

Étude de cas technique contextualisée

A partir d'une situation de mise en production d'une solution blockchain (smart contracts + DApp), le candidat doit analyser la situation, identifier les actions correctives à mener, proposer des améliorations, et démontrer sa capacité à maintenir la solution dans des conditions opérationnelles.

Modalités de mise en oeuvre :

Étude de cas individuelle, à réaliser en 3h

RNCP41719BC05 — Intégrer les principes de durabilité et de sobriété numérique dans le développement et le déploiement de solutions blockchain

LISTE DE COMPÉTENCES

Évaluer et intégrer les impacts environnementaux d'une solution blockchain en analysant la consommation énergétique, les émissions carbone, les effets de redondance des architectures distribuées et les contraintes liées au cycle de vie des données,

Éco-concevoir les composants d'une solution blockchain en identifiant les sources principales de consommation de gas ou de ressources dans le développement des smart contracts et des DApps, en optimisant la logique algorithmique et la structure du code, et en appliquant des principes d'écoconception adaptés aux environnements décentralisés,

Mettre en oeuvre des pratiques DevOps éco-responsables dans le déploiement de solutions blockchain en limitant les redondances et la fréquence des livraisons, en sélectionnant des infrastructures d'hébergement ou de cloud à faible empreinte carbone, et en configurant les environnements d'exécution de manière sobre et efficiente,

Contribuer à l'intégration de la sobriété numérique dans la stratégie RSE appliquée aux projets blockchain en participant à la définition d'indicateurs environnementaux pertinents, en identifiant les leviers d'alignement entre les choix techniques et les engagements de l'organisation, et en appuyant les démarches de sensibilisation ou d'amélioration continue,

Aligner les pratiques de développement blockchain sur les référentiels et normes du numérique responsable en analysant les exigences des cadres réglementaires et sectoriels (RGESN, REEN, Green IT, ISO 14001...), en identifiant les écarts de conformité et en mettant en oeuvre les ajustements nécessaires, y compris dans le cadre de démarches de certification ou de labellisation,

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée à partir d'un projet blockchain réel ou fictif.

Étude de cas professionnelle

Le candidat est évalué sur sa capacité à analyser les impacts environnementaux des choix techniques réalisés, à identifier des leviers d'optimisation concrets portant sur le code, les outils ou l'infrastructure, à formuler des recommandations d'écoconception adaptées au contexte blockchain, et enfin à proposer des mesures d'alignement avec une stratégie RSE.

Modalités de mise en oeuvre

Étude de cas individuelle à réaliser en 3 heures

Remise d'un dossier structuré

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le concepteur développeur de solutions blockchain peut exercer son activité dans des secteurs variés tels que la finance (cryptomonnaies, paiements, assurances), la logistique et la supply chain (traçabilité, certification), l'énergie (échanges décentralisés), l'industrie (sécurisation des données et automatisation), la santé (gestion sécurisée des données médicales), ou encore les services numériques (identité numérique, gestion documentaire, applications décentralisées), au sein d'entreprises technologiques, de start-ups spécialisées, de cabinets de conseil ou de directions innovation de grands groupes.

TYPE D'EMPLOIS ACCESSIBLES

Développeur blockchain responsable - Développeur blockchain - Concepteur blockchain

RÈGLEMENTATIONS D'ACTIVITÉ

Bien qu'il ne s'agisse pas d'une profession ou métier non réglementé, le développeur blockchain responsable doit cependant exercer ses activités dans le respect d'un cadre légal et réglementaire assez vaste qu'il doit impérativement intégrer à chaque étape du développement.

Les principales réglementations à prendre en compte sont :

- Règlement général sur la protection des données (RGPD)
- Règlement MiCA (Markets in Crypto-Assets)
- Règlement eIDAS 2 (identité numérique européenne)
- Directive NIS 2 et Cyber Resilience Act (sécurité des systèmes d'information)
- Accessibilité numérique : RGAA (Référentiel général d'amélioration de l'accessibilité) et WCAG
- Cadres de sobriété numérique et RSE (Loi REEN (Réduction de l'empreinte environnementale du numérique, Référentiel général d'écoconception des services numériques (RGESN)...),

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Très élevée (5/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 4 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 864 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (41 % des actifs en emploi)
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique · tension 4/5 (Élevée) M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	27 458
Jugés difficiles à recruter	53 %
Emplois saisonniers	1 %
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom

Voies d'accès

MODALITÉS D'ACCÈS

Formation initiale, Formation continue, Apprentissage, Contrat de professionnalisation, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Justifier d'un diplôme ou titre de niveau 5 dans les domaines suivants : Informatique / SI, Numérique / développement , Connaissances en programmation (Python, JavaScript, etc.) , Compréhension des architectures web , Appétence pour les enjeux de cybersécurité et d'innovation technologique

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION, VAE

Le jury de certification est composé de trois membres :

- 2 professionnels qualifiés, extérieurs au certificateur, habilités pour leur expertise sur le métier et ayant exercé ou encadré des professionnels dans des fonctions similaires à celles de développeur blockchain responsable ou une

activité similaire. L'un des membres est président

- 1 représentant du certificateur

Base légale

Date de décision	27/10/2025
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	27/10/2028
Date de dernière délivrance possible	26/10/2032

Liens avec d'autres certifications

CORRESPONDANCES (PAR BLOCS)

RNCP37778, RNCP40166

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/41719/>

Où se former

Formations référencées	7
Organismes	1
Régions couvertes	1
Prix indicatif	1 395 € – 9 948 €
Durée	38 – 84 h

Offre de formation — MonCompteFormation (Caisse des Dépôts), licence ouverte.

Demande CPF — formations engagées

Dossiers CPF engagés	1
Montant total engagé	5 290 €
Coût moyen par dossier	5 290 €
Durée moyenne	84 h
Période	03/2026
France compétences	93 %
Reste à charge titulaire	7 %

Formations engagées via le CPF — Caisse des Dépôts (open data), tous organismes confondus.